Canadian Heritage | Patrimoine canadien

Canada

Information and Records Management Audit

Office of the Chief Audit and Evaluation Executive
Audit and Assurance Services Directorate

September 2011

Cette publication est également disponible en français.

This publication is available upon request in alternative formats.

This publication is available in PDF and HTML formats on the Internet at http://www.pch.gc.ca

Catalogue No. CH6-7/2011E-PDF
ISBN: 978-1-100-20177-1

Table of Contents

Executive Summary

Introduction

The objective of this audit is to provide assurance on the adequacy and effectiveness of the control framework at the Department of Canadian Heritage (PCH) to manage and protect information in accordance with relevant acts, Treasury Board Secretariat (TBS) and Departmental policies, procedures and practices.

The Department is responsible for formulating policies and delivering programs related to Canadian identity and values, cultural development, and heritage. Information is an essential component of effective management. It supports the delivery of programs and services and enables PCH to be more responsive and accountable to Canadians. The information managed by the Department is as varied as the initiatives and activities undertaken to meet the Department's mandate. This includes information related to grants and contributions (G&Cs) (e.g., correspondence, applications), corporate services (e.g., HR, policy development, analysis and research), and the operations of the Department (e.g., business plans, reports).

The Knowledge and Information Management Directorate (KIM) within the Chief Information Officer Branch (CIOB), has the mandate to provide the strategic direction, tools, and guidance related to the appropriate management of information within the Department, including the development of the Department's Information Management (IM) Policy.

All employees of the Department are responsible for applying IM principles, standards, and practices in the performance of their duties, and for documenting their activities and decisions. IM resources outside of KIM vary across branches and sectors, related to resource level, role, and classification. In some branches, there is an assigned position that is responsible for IM, while in others, an individual may have part time IM responsibilities. In general, staff with IM responsibilities outside of the KIM Directorate act in a 'record management' role focused on the managing of hardcopy records, than that of an IM Specialist.

The majority of information at PCH resides and is managed at the program level, in both electronic and hardcopy form. While active hardcopy records generally reside with the program areas, a corporate Records Office managed by KIM is used to store inactive and/or dormant files. However the process to manage this information is intensively manual.

The findings resulting from this audit should be viewed in the context of current IM-related developments, both within PCH and the broader federal government environment that may have a significant impact on PCH's IM Strategy and the audit's findings and recommendations. Specifically, this includes:

- The Grants and Contributions Modernization Initiative (GCMI) is intended to standardize and rationalize G&C processes across the Department, including upgrading current G&C systems (i.e. GCIMS). This initiative commenced in Spring 2010 and is expected to be completed by 2013, and will have a significant impact on the IM practices of G&C programs.
- The current fiscal environment, for example, the Strategic Review of the operating expenses of government institutions, the federal government's deficit reduction action plan, Administrative Services Review and the Internal Services Review means that available resources may be constrained and additional IM resources may not be available.
- The Government of Canada (GC), through the new Shared Services Canada entity is intending to streamline and consolidate federal government IT infrastructure and operations, particularly email, data centres and networks.
- Federal government institutions have until Spring 2014 to implement the requirements of the TBS Directive on Recordkeeping. 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.
- The Treasury Board Secretariat has started developing standards in relation to IM roles and responsibilities and plans to create generic IM job descriptions.

Key Findings

Strengths

During the audit fieldwork, the audit team observed several examples of how controls related to IM are properly designed and being applied effectively. This resulted in positive findings, including:

- A PCH IM Policy has been in effect since April 1, 2010. This policy outlines roles and responsibilities for IM within the Department, consistent with the Treasury Board Policy on Information Management and Directive on IM Roles and Responsibilities.
- The processes and response time to Access to information (ATI) requests has been greatly improved over the past year.
- Certain areas across the Department have initiated a 'clean-up' of their network drives.
- The PCH Intranet contains some IM resources that are available for staff to review.

- Information of business value is being identified and retained by program areas; for many program areas, this is achieved through the use of standard forms and processes.

Observations

The audit team also identified areas where management practices and processes can be improved. The following are observations made by the audit team that highlight areas of improvement that should be addressed by PCH.

1. The 2011-2016 IM Strategy, in its current draft form, contains objectives, initiatives, and timelines that need to be aligned with current resource levels, prioritized and consulted on with departmental stakeholders and PCH's IM-related governance committees.
2. Coordination and outreach between KIM and PCH branches/regions related to roles and responsibilities for IM, collaboration on IM-related initiatives, and the dissemination and training of IM standards and practices are infrequent given resources constraints and competing priorities.
3. A comprehensive suite of IM-related standards, practices and tools need to be developed to support PCH's IM Policy. IM practices, including the classification and organization of information is inconsistent throughout the Department.
4. Record Disposition Authorities (RDAs) for approximately half of the 100 PCH programs/units that have been identified as requiring RDAs for the program-specific records in which they manage have to be obtained.

   Information is being retained for longer than required, especially records that are in electronic format.
5. Standards for the security classification of information, and the appropriate safeguards to protect sensitive information, are inconsistent and/or are not being applied.

Recommendations

1.1. The Chief Information Officer (CIO) should actively engage the Department's governance committees for input into the current draft IM Strategy, and considering available resources, specifically prioritize objectives/ initiatives, including a performance measurement plan, with a consideration of the risks to the Department of not achieving specific objectives in the Strategy.

The following audit findings in this report also provide an indication of IM areas that present risks to the Department and that should be considered when determining priorities in the Strategy.

In setting priorities in the IM Strategy, the CIO should consider:

2.1. Engaging branches/regions to define current IM capabilities and capacity within the branches/regions, and enabling further collaboration to ensure these IM resources can be effectively utilized. Activities should be intended to help position the Department to further standardize IM resource roles.

2.2. Ensuring the KIM further collaborates with the Access to Information Privacy (ATIP) Secretariat and Departmental Security to establish formal mechanisms for considering IM requirements during the assessment and development of privacy and security controls throughout PCH.

3.1. Prioritizing the completion of the information architecture for the Department, with an initial focus on the classification of records throughout the Department, regardless of format or medium.

4.1. Determining the extent to which more generic RDAs can be utilized for program areas that currently do not have an approved RDA, in order to reduce the number of RDAs for which approval is required. The process standardization work of the GCMI could be leveraged in this context.

4.2. Assisting program areas in identifying information that is no longer of business value. This should include the development of strategies in collaboration with program areas on the disposition of information that is stored in electronic databases.

In setting priorities in the IM Strategy, the CIO, in collaboration with the Departmental Security Officer and the ATIP Coordinator, should consider:

5.1. Ensuring that the development of the information architecture for the Department includes considerations related to the security classification of information, as well as ensuring there are appropriate safeguards implemented, and tools available, for the management of classified information. This includes conducting Threat and Risk Assessments (TRAs), for example on the corporate Records Office, and Privacy Impact Assessments (PIAs), for example, on the PeopleSoft upgrade.

5.2. Ensuring additional training and awareness on the security classification of information is provided to staff, focused on appropriate safeguards based on the level of sensitivity of the information being managed.

Statement of Assurance

In my professional judgment as Chief Audit and Evaluation Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed to with management. The opinion is applicable only to the entity examined and within the scope described herein. The evidence was gathered in compliance with Treasury Board policy, directives, and standards on internal audit. Sufficient evidence was gathered to provide senior management with the proof of the opinion derived from the internal audit.

Audit Opinion*

In my opinion, the IM governance, risk and control framework at PCH to manage and protect information in accordance with relevant acts, TBS and Departmental policies, procedures and practices has control weaknesses with moderate risk exposures that require management attention, related to strategy; roles and responsibilities; standards, practices and tools; and the safeguarding of information relative to the IM control framework.

Original signed by :

_____

Richard Willan
Chief Audit and Evaluation Executive
Department of Canadian Heritage

Audit Team Members

Maria Lapointe-Savoie
Dylan Edgar
Siriseng Malichanh
Yves Christian
Caroline Dulude
With the assistance of external resources

* The audit opinion is based on overall materiality and risk as represented by the noteworthy findings and recommendations reported.

1. Introduction and Context

1.1 Authority for the Project

The authority for this audit is derived from the Multi-Year Risk-Based Audit Plan (RBAP) 2011-2012 to 2013-2014 which was recommended by the Departmental Audit Committee (DAC) and approved by the Deputy Minister in March 2011.

1.2 Background

The Department of Canadian Heritage (PCH) is responsible for formulating policies and delivering programs related to Canadian identity and values, cultural development, and heritage. This mandate is met through a wide range of varied activities and initiatives, involving diverse information holdings, including those related to copyright, foreign investment and broadcasting, the arts, culture, heritage, official languages, sports, state ceremonial and protocol. Information is an essential component of effective management; for example, accurate and timely information is necessary for appropriate management decision making. This includes decisions on policy and program design/delivery, and Departmental reporting to Government of Canada (GC) central agencies. It supports the delivery of programs and services and enables PCH to be more responsive and accountable to Canadians.

The Knowledge and Information Management Directorate (KIM) within the Chief Information Officer Branch (CIOB) has the mandate to provide the strategic direction, tools, and guidance related to the appropriate management of information within the Department, including adherence to federal government information management (IM) requirements such as the *Library and Archives of Canada Act* and the Treasury Board Secretariat (TBS) Policy on Information Management and Directive on Recordkeeping.

The KIM has 15 positions, each currently staffed. Since 2007, the position count has increased from 10 to 15. The Directorate is composed of the following units:

- IM/KM (Information Management/Knowledge Management) Strategies and Change Management - Key activities of the unit include strategic planning, policy development, performance measurement and IM communications and awareness.
- IM Client Services - The unit provides operational support and training to PCH employees that address IM life cycle requirements, including supporting current users of InfoCentre and Integrated Recorded Information Management System (iRIMS), and answering inquiries through an IM Help Desk. The corporate Records Office is a sub-unit of IM Client Services.
- Knowledge Centre - The unit is a multi-functional, single-window to information and knowledge services, including library services. The unit includes the Learning and Conference Centre (LCC), a dedicated space for training and learning for the Department. These services were not included in the audit.

All PCH employees are responsible for applying information management principles, standards, and practices in the performance of their duties, and for documenting their

activities and decisions. Positions with IM responsibilities and IM resources outside of KIM vary across branches and sectors, related to resource level, role, and classification. In some branches, there is an assigned position that is responsible for IM, while in others, an individual may have part time IM responsibilities. In general, staff with IM responsibilities outside of KIM act in a 'record management' role focused on the managing of hardcopy records, than that of an IM Specialist.

The majority of information at PCH resides and is managed at the program level, in both electronic and hardcopy form. The main electronic information repositories include:

- Email (Lotus Notes);
- Corporate network drives (for example, the 'G: drive');
- InfoCentre (Electronic Document and Record Management System (EDRMS));
- Corporate applications such as PeopleSoft (HR system), Grants and Contributions Information Management System (GCIMS), and CCM Mercury; and,
- Numerous program-specific applications.

The same information is often in several places and formats. For example, G&C related information such as program application forms and program correspondence is often managed through email, documents or databases on the network drive, GCIMs, and/or hardcopy files. The vast majority of program areas still retain paper records as they need signed copies, as PCH considers 'signed originals' as the official record. As such, the process to manage this information is intensively manual.

Although active hardcopy records generally reside with program areas, there is also a corporate Records Office managed by KIM where inactive and/or dormant files are stored. The Directorate utilizes Integrated Recorded Information Management System (iRIMS) to manage hardcopy records within its corporate Records Office.

2. Objective

The objective of this audit is to provide assurance on the adequacy and effectiveness of the control framework at PCH to manage and protect information in accordance with relevant acts, TBS and Departmental policies, procedures and practices.

3. Scope

The scope of this audit includes all information managed by PCH, regardless of format (i.e., paper, electronic) and covers the management of information across the IM lifecycle, as defined by Library and Archives Canada (LAC):

1. IM planning;
2. Collection, Creation, Receipt and Capture;

3. Organization of Information;
4. Use and Dissemination;
5. Maintenance; Protection and Preservation
6. Disposition; and,
7. Evaluation and Monitoring.

4. Approach and Methodology

The approach and methodology for the audit were consistent with Treasury Board *Policy on Internal Audit and* related internal auditing standards for the Government of Canada.

PCH strives to maintain an IM control framework that is reflective of central agency requirements and industry leading practices. Consequently, IM-related requirements of the *Privacy Act*, the *Access to Information Act* and the *Library and Archives of Canada Act* were leveraged for this audit. In addition to these three statutes, IM-related requirements were considered related to the following TBS policies and directives:

- Policy on Information Management
  - Directive on Information Management Roles and Responsibilities
  - Directive on Record Keeping
- Policy on Privacy Protection and related Directives
- Policy on Access to Information and related Directives
- Policy on Government Security

Audit activities were performed within the CIOB (specifically KIM), as well as specific branches/regions throughout PCH in order to assess if effective IM practices have been implemented throughout the Department. Specific areas were selected for audit activity through the preliminary assessment (i.e., planning phase) conducted for the audit. Areas were selected given their inherently high risk information holdings, as well as to ensure a representative sample of branches based on the particularities of their current IM practices. The following areas within PCH were the focus of the audit:

- Aboriginal Affairs Branch (AAB);
- Cultural Sector Investment Review (CSIR);
- Canadian Heritage Information Network (CHIN);
- Human Resources and Workplace Management (HRWM) ;
- PAN AM 2015 Secretariat (use of InfoCentre);
- Access to Information and Privacy (ATIP);
- Atlantic Region;
- Ontario Region; and,
- Major Events and Celebrations Branch (MEC).

Audit procedures performed within these areas included:

- Review of IM related policies, procedures, standards, and assessments;
- Review of IM and Branch-specific strategic and business plans, oversight committees' terms of reference, and meeting minutes;
- 47 interviews and process walkthroughs with PCH employees and management related to IM practices; and,
- Examination, review and analysis of information repositories (i.e., hardcopy files, network drives, and electronic databases).

The application of these procedures was intended to allow the formulation of a conclusion as to whether the audit criteria established for this audit were being met. Evidence was gathered in compliance with Treasury Board policy, directives, and standards on internal audit. Standards for evidence were followed to ensure that information is sufficient, reliable, relevant, and useful to draw conclusions and meet the objectives of the audit.

5. Findings and Recommendations

Based on interviews, analysis, and evidence gathered throughout the audit, each audit criterion was assessed by the audit team and conclusions are included in Appendix A.

Information and records management controls were found to be properly designed and being applied effectively in specific areas; and, the audit team identified opportunities for improvement resulting in eight recommendations in the areas of IM governance, internal controls and risk management.

5.1 IM Strategy

> The 2011-2016 IM Strategy, in its current draft form, contains objectives, initiatives, and timelines that need to be aligned with current resource levels, prioritized and consulted on with departmental stakeholders and PCH's IM-related governance committees.

Analysis

An Information Management (IM) Strategy was initially developed in 2007 to cover a five-year period from 2007 to 2012, and was updated in 2010. This previous strategy had input and approval from PCH senior management. The Knowledge and Information Management Directorate (KIM) determined a new strategy was required, and a draft PCH IM Strategy is currently under development that presents the direction that the Departmental IM agenda will take from 2011 to 2016. Several strategic objectives (16 in total) have been identified related to the Strategy's five strategic goals. The timelines associated with these objectives indicate a substantial amount of work to begin in 2011-12, with work completed by end of fiscal year 2013-14, including the development of an IM Performance Measurement Strategy.

The focus of the first four strategic goals and their related objectives/initiatives are related to recordkeeping, as the strategy is intended to serve as a roadmap to address the 2014 compliance requirements of the TBS Directive on Recordkeeping. The fifth strategic goal, to "*Foster Knowledge and Collaboration Channels*", is less related to recordkeeping, and contains seven of the plan's 16 objectives. These objectives have yet to be prioritized within the Strategy, however key risks have been presented, and the strategies intended to mitigate these risks have been identified.

KIM has indicated that PCH currently does not have the resources required to achieve the objectives in the draft IM Strategy. An external assessment commissioned by the CIOB further indicated that in order for PCH to ensure compliance with the TBS Directive on Recordkeeping, there is a need to improve the capacity and capabilities of IM Specialists

within the Directorate. Considering the current fiscal environment, it is not likely that all required resources to meet the objectives of the IM Strategy will be provided.

The current IM Strategy still needs to be discussed at PCH's IM-related governance committees in 2011, either the level 3 Business Operations Committee (BOC) or level 4 Enterprise Architecture Committee (EAC). Of note, the Departmental IM governance framework has recently been modified, and these committees have only recently established their mandates and meeting schedule.

Risk Assessment

A comprehensive IM Strategy should consider Departmental resource constraints and other risks of not achieving objectives, such as compliance to legislative and policy requirements, in order to prioritize objectives/initiatives. This ensures that Senior Management is aware of the risks related to the non-achievement of the objectives of the IM Strategy and is able to provide well-informed input into IM resource allocation decisions. Senior Management input increases the likelihood of the objectives outlined within the IM Strategy being achieved.

Recommendation

The Chief Information Officer (CIO) should:

1.1. Actively engage the Department's governance committees for input into the current draft IM Strategy, and considering available resources, specifically prioritize objectives/initiatives, including a performance measurement plan, with a consideration of the risks to the Department of not achieving specific objectives in the Strategy.

The following audit findings in this report also provide an indication of IM areas that present risks to the Department and that should be considered when determining priorities in the Strategy.

5.2 IM outreach/training and IM roles/responsibilities

Coordination and outreach between the KIM and PCH branches/regions related to roles and responsibilities for IM, collaboration on IM-related initiatives, and the dissemination and training of IM standards and practices are infrequent given resources constraints and competing priorities.

Analysis

Given resource constraints relative to the current environment facing the Department and an inward focus related to KIM-driven initiatives such as policy development, the Directorate decided to only provide ad hoc IM support to the operations of program and branch/regional activities within the Department. This includes limited IM training and awareness provided to departmental staff. Some IM-related training is provided in new employee orientation sessions. Ad-hoc IM-related training is also provided by KIM based on requests from program areas. An IM training strategy and plan has yet to be developed.

IM resources outside of KIM vary across branches and sectors, related to resource level, role, and classification. In some branches, there is an assigned position that is responsible for IM, while in others, an individual may have part time IM responsibilities. In general, staff with IM responsibilities outside of KIM act in a 'record management' role focused on managing hardcopy records, rather than that of an IM Specialist.

Although an IM Community of Practice has been established for IM practitioners throughout the Department, collaboration between KIM and the branches/regions is infrequent. Contributing factors consist of the variation in the profiles of resources across the Department as well as a shortage of formal IM standards and tools developed by the KIM for use within program areas.

Through the new PCH governance structure for IT-enabled projects, KIM is liaising with the ATIP Secretariat and Departmental Security on matters relating to IM, privacy, and security requirements.

Risk Assessment

Well-defined roles and responsibilities and appropriate outreach reduce the risk of PCH not being compliant with Government of Canada (GC) IM requirements, specifically the requirements of the Directive on Recordkeeping, which is required by 2014. Well defined roles and responsibilities further ensure IM practices are consistent between program areas, making the integration of programs into corporate wide IM initiatives such as a new classification structure and/or an Electronic Document and Records Management System (EDRMS) solution less difficult and resource intensive. This also furthers the efficient and effective sharing of information within the Department and increases the likelihood of the objectives outlined within the IM Strategy being achieved.

Recommendations

In setting priorities in the IM Strategy, the CIO should consider:

2.1. Engaging with branches/regions to define current IM capabilities and capacity within the branches/regions, and enabling further collaboration to ensure these IM resources can be effectively utilized. Activities should be intended to help position the Department to further standardize IM resource roles.

2.2. Ensuring KIM further collaborates with the ATIP Secretariat and Departmental Security to establish formal mechanisms for considering IM requirements during the assessment and development of privacy and security controls throughout PCH.

5.3 IM Standards, Practices, and Tools

A comprehensive suite of IM-related standards, practices and tools need to be developed to support PCH's IM Policy. IM practices, including the classification and organization of information is inconsistent throughout the Department.

Analysis

A new PCH IM Policy has been in effect since April 1, 2010. This policy outlines roles and responsibilities for IM within the Department, consistent with the TB Policy. A comprehensive suite of IM-related standards and guidelines to support the IM Policy has yet to be been developed; this includes specific guidance or standards related to data sharing. In general, there were few instances of data sharing with government partners and stakeholders identified during the audit although where data sharing was identified, formal agreements were not in place.

The PCH Intranet contains some IM reference material available for staff to review. This material includes an 'IM Quick Reference Card', 'Best Practices for Clean Up of the Shared Drive', and 'Information Protection and Classified Guide'. These resources are not well known and the content is not well understood by staff as IM awareness and/or guidance program to provide context and/or training on the use of these resources is not in place.

Information of business value is being identified and retained by program areas; however, information of a more transitory nature and/or not of operational value is also being collected at the same time, and subsequently being retained and not differentiated from the information of business value. This information is often related to day-to-day operations and collaboration within programs via emails and on network drives.

The same information is often in several places and formats. For example, G&C related information such as program application forms and program correspondence is often managed through email, documents or databases on the network drive, GCIMs, and/or

hardcopy files. Program areas still retain paper records, as PCH considers ‘signed originals’ as the official record.

The Department utilizes a classification system using iRIMs for hardcopy records. Some program areas would be well-served by additional clean-up of iRIMs entries of hardcopy records. This classification system is not consistently used with hardcopy records throughout the Department. Regional offices visited have created their own ad hoc records classification systems.

There is a need to develop a standard classification for information in electronic format or medium such as information in network drives or databases. Networks drives are inconsistently organized throughout the Department, and the information within these drives are inconsistently labelled (i.e., through naming conventions) or managed. There are no coherent standards for the naming of electronic documents. In consideration, PCH has initiated an Information Architecture/Classification Project, with the objective to build an information architecture/classification structure for the Department, applicable not only to an eventual Electronic Document and Record Management System (EDRMS) implementation, but to other information repositories throughout the Department. A Conceptual Classification Model has been established as part of this project.

A pilot EDRMS implementation (InfoCentre) has been in place within the Department since 2006, specifically used with the 2010 Olympic and Paralympic Games Federal Secretariat (from 2007 to 2010). InfoCentre is also being used by the executive correspondence management community (via integration with the CCM Mercury tracking application) since 2008. Additional pilot projects are still in effect, including with the 2015 Pan Am Games Secretariat and within the CIOB. For InfoCentre users, there are no standard procedures provided and classification and naming conventions are not consistent between pilot areas. The current expansion of this pilot project has been stopped. CIOB is currently developing a business case for the corporate implementation of a new EDRMS solution.

The Grants and Contributions Information Management System (GCIMS) is not being consistently utilized by G&C program areas. Each program area has developed their own standards for the information that may be placed in GCIMS and how it may be organized. It was noted that GCMI is intended to further standardize G&C processes.

Risk Assessment

The development and dissemination of IM standards, practices, and tools throughout the Department, increases the likelihood that PCH will be compliant with Government of Canada IM requirements, specifically the requirements of the Directive on Recordkeeping, which is required by 2014. Defined IM standards, practices and tools further ensure IM practices are consistent between program areas, making the integration of programs into corporate wide IM initiatives such as a new classification structure and/or EDRMS solution less difficult and resource intensive. This also furthers the efficient and effective sharing of information within the Department.

Ensuring that information without business value is removed in a timely manner ensures the optimal use of resources (infrastructure capacity, storage costs for hardcopy records, and record management staff related to the managing of hardcopy records). Not having to consider extraneous information facilitates the ability to respond in a timely manner to Access to Information (ATI) requests or complete information discovery related to litigation. The more information relating to these events that is classified in a structured fashion to search and/or hold impacts the number of resources and time required to respond to these requests.

Recommendation

In setting priorities in the IM Strategy, the CIO should consider:

3.1. Prioritizing the completion of the information architecture for the Department, with an initial focus on the classification of records throughout the department, regardless of format or medium.

5.4 Retention and Disposition Practices

Record Disposition Authorities (RDAs) for approximately half of the 100 PCH programs/units that have been identified as requiring RDAs for the program-specific records in which they manage have to be obtained.

Information is being retained for longer than required, especially records that are in electronic format.

Analysis

PCH holds a number of institution-specific RDAs from Library and Archives Canada (LAC) covering its information resources collections up to the early 1990's. KIM is currently working with program areas and LAC to obtain additional RDAs. Approximately half of the 100 PCH programs/units identified by KIM as requiring institution-specific RDAs have yet to obtain a RDA. PCH is utilizing Multi-Institutional Disposition Authority (MIDA) where possible to dispose of records. This authority relates 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.

The audit team noted that electronic records are not being consistently disposed of. For example:

- Corporate databases such as GCIMS and PeopleSoft and those used within specific programs have retained information indefinitely, meaning information from the late 1990s remains available through these systems.
- Network drives within program areas have not been subject to formal disposition processes, and information of no business and/or operation value was identified by the audit team (e.g., draft reports from the mid-1990s).

The audit team noted that hardcopy records related to specific program activities (e.g., G&C programs) were being regularly considered for disposition. Hardcopy records related to other business activities, such as the administration of programs (i.e., planning, reports, policies, etc.) were not subject to such a formal disposition process. Examples of information that had no operational value were noted in program area records rooms that had information dating back to over five years where normally these records would have migrated to the corporate Records Room. PCH staff indicated that in many cases they had switched to filing information on the network drive, and had left the hardcopy file 'as is' within the file room.

Risk Assessment

RDAs are required to be obtained in order to legally dispose of information. Ensuring that information is disposed of in a timely manner ensures the optimal use of resources (infrastructure capacity, storage costs for hardcopy records, and record management staff related to the managing of hardcopy records). Not having to consider extraneous information facilitates the ability to respond in a timely manner to Access to Information (ATI) requests or complete information discovery related to litigation. The greater amount of information to search and/or hold related to these events impacts the number of resources and time to respond to these requests.

Appropriate retention and disposition practices will serve well to comply with the requirements of the Directive on Recordkeeping, which is required by 2014.

Recommendations

In setting priorities in the IM Strategy, the CIO should consider:

4.1. Determining the extent to which more generic RDAs can be utilized for program areas that currently do not have an approved RDA, in order to reduce the number of RDAs for which approval is required. The process standardization work of the GCMI could be leveraged in this context.

4.2. Assisting program areas in identifying information that is no longer of business value. This should include the development of strategies in collaboration with program areas on the disposition of information that is stored in electronic databases.

5.5 Protection of Sensitive Information

Standards for the security classification of information, and the appropriate safeguards to protect sensitive information, are inconsistent and/or are not being applied.

Analysis

Despite well received, although limited, security classification training provided throughout the Department, the security classification of information is not consistently applied. In our sample, information that should have been classified was often not marked as such and was stored in an unclassified file. The audit notes that when information was being marked as sensitive/confidential, there was no indication of the specific classification level of the information (e.g. Protected A or B)

Information that should be considered Protected B is being emailed unencrypted as well as being managed within the Department network drive and found in GCIMS, which are intended to only transmit/manage information up to Protected A. Access controls related to the information managed in the Department network drive are difficult to maintain, given the need to manage access to different folders. In certain cases, the network folder for a branch is available to anyone within the branch.

The corporate Records Office managed by KIM has not specifically segregated records based on level of sensitivity, and Secret documents are stored in the same area as other less sensitive records. A formal assessment of the Records Office safeguards has not been conducted.

PCH has yet to develop a formal Privacy Management Framework for the Department to identify and mitigate privacy risks and help ensure compliance with *Privacy Act* and related Treasury Board requirements. A component of this framework would be the assessment and management of privacy risks, through the conduct of Privacy Impact Assessments (PIAs). For instance, the current PeopleSoft application has not been subject to a PIA, nor is the planned PeopleSoft upgrade expected to have a PIA performed.

Risk Assessment

An appropriate privacy management framework or standards for the security classification of information mitigate the risk that safeguards with the sensitivity of the information will not be implemented. The absence of a framework increases the risk of the inappropriate use and disclosure of sensitive information, which may lead to a privacy and/or security breach or incident, including non-compliance with the *Privacy Act* or Policy on Government Security; and increases the risk of critical information being subject to an unauthorized modification or deletion.

Recommendations

In setting priorities in the IM Strategy, the CIO, in collaboration with the Departmental Security Officer and the ATIP Coordinator, should consider:

5.1. Ensuring that the development of the information architecture for the Department includes considerations related to the security classification of information, as well as ensuring there are appropriate safeguards implemented, and tools available, for the management of classified information. This includes conducting Threat and Risk Assessments (TRAs), for example on the corporate Records Office, and PIAs, for example, on the PeopleSoft upgrade.

5.2. Ensuring additional training and awareness on the security classification of information is provided to staff, focused on appropriate safeguards based on the level of sensitivity of the information being managed.

Appendix A – Audit Criteria

The conclusions reached for each of the audit criteria used in the audit were developed according to the following definitions.

Numerical Categorization	Conclusion on Audit Criteria	Definition of Conclusion
1	Well Controlled	• well managed, no material weaknesses noted; and • effective.
2	Controlled	• well managed, but minor improvements are needed; and • effective.
3	Moderate Issues	Has moderate issues requiring management focus (at least one of the following two criteria need to be met): • control weaknesses, but exposure is limited because likelihood of risk occurring is not high; • control weaknesses, but exposure is limited because impact of the risk is not high.
4	Significant Improvements Required	Requires significant improvements (at least one of the following three criteria need to be met): • financial adjustments material to line item or area or to the department; or • control deficiencies represent serious exposure; or • major deficiencies in overall control structure. Note: Every audit criteria that is categorized as a **"4"** must be immediately disclosed to the CAEE and the subjects matter's Director General or higher level for corrective action.

The following are the audit criteria and examples of key evidence and/or observations noted which were analyzed and against which conclusions were drawn. In cases where significant improvements (4) and/or moderate issues (3) were observed, these were reported in the audit report, and the exposure risk is noted in the table below.

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
1. IM Planning			
1.1 - Governance structure, roles & responsibilities and strategies for IM are defined, assigned, and communicated throughout PCH.			
1.1.1	An IM governance and accountability framework has been established that ensures Senior Management discusses IM on a regular basis and provides sufficient oversight of IM related to leadership, visioning, and funding.	**2**	A new IM governance and accountability framework has recently been established that is appropriately designed; although the operating effectiveness of its oversight cannot be determined yet given the preliminary nature of the governance framework.
1.1.2	Roles and responsibilities for IM have been defined, assigned and communicated for all staff.	**3**	Resourcing for IM staff varies across the Department. In some branches, there is an assigned position that is responsible for IM, while in others, an individual may have part time IM responsibilities. These positions are not standardized throughout the Department, either in terms of classification or roles/ responsibilities.
1.1.3	IM strategic plans are aligned with Departmental priorities and address IM risks and legislative and policy requirement.	**3**	The IM Strategy, in its current draft form, contains objectives, initiatives, and timelines that are not aligned with current resource levels. These objectives/initiatives have not been subject to prioritization, nor have the risks related to not achieving these objectives been outlined within the Strategy. Furthermore, input into the Strategy has not yet been formally sought from PCH's IM-related governance committees or other areas of the Department to help prioritize initiatives and identify risks.

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
1.1.4	Branch/Sector/Regional operational plans include IM requirements.	**3**	IM considerations have been included within the PCH Integrated Business Plan (IBP) template; however, planning within branches/ regions, when IM was considered, has only considered IM requirements/ risks at a high level.
1.1.5	HR capacity and capabilities related to IM are sufficient to meet the needs of the organization.	**3**	Interviewed PCH staff have indicated that to ensure compliance with the TBS Directive on Recordkeeping, it would need to improve the capacity and capabilities of IM Specialists within KIM. Resourcing for IM staff varies across the department. In general, there are no dedicated IM specialists within PCH branches. An assessment of IM capabilities and requirements within program areas or regions has not been undertaken by the Department.
1.2 - A comprehensive policy framework has been established, and is supported by appropriate procedures and guidelines, as well as by a training and awareness program.			
1.2.1	IM policies and guidance based on legislative and policy requirements have been developed, implemented, communicated, and reviewed regularly.	**3**	A new PCH IM Policy has been in effect since April 1, 2010. This policy outlines roles and responsibilities for IM within the Department, consistent with the TB Policy. A comprehensive suite of IM-related standards and guidelines to support the IM Policy has not been developed, although the KIM Directorate has initiated the IM Policy Suite Project, and has been tasked with developing IM policy instruments, such as standards and guidelines.
1.2.2	Procedures and guidelines have been established to ensure adherence to IM policies within branches/regions areas.	**3**	Branches/regions have varying levels of standards related to IM, although some have been formally documented, many have not been. Standards and practices are not consistent throughout the Department.

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
1.2.3	A process has been implemented to ensure all PCH staff receives appropriate IM training and awareness based on their job position, including during new hire orientation.	**3**	An IM training strategy and plan has not been developed. KIM has initiated several ad hoc IM awareness related activities; however, there has still been limited involvement with branch/region staff related to IM awareness and requirements.
2. Collection, Creation, Receipt and Capture			
2.1 - Formal procedures and guidelines have been developed and are followed to ensure information is assessed at time of creation related to its role and business value.			
2.1.1	A process has been implemented to assess information for its role and business value at time of creation, and information is collected in compliance with the requirements of the *Privacy Act*.	**3**	Information of business value is being identified and retained by program areas; however, there is no standard processes for ensuring only information of business value is being collected/created and retained, information of a transitory nature and/or of no operational business value was identified throughout the branches/regions.
3. Organization of Information			
3.1 - Information repositories (electronic/ hardcopy) have been designated to maintain information resources of business value.			
3.1.1	Information repositories have been appropriately established and are being utilized	**2**	There are no formal standards for the establishment of information repositories; however repositories are being utilized throughout PCH for the management of information of business value.
3.1.2	A process has been established to ensure electronic information repositories are the preferred method of storage.	**3**	The vast majority of program areas still retain paper records, as PCH considers 'signed originals' as the official record. An EDRMS was rolled out on a pilot fashion but the current strategy for implementing a solution in on hold, awaiting a new business case.
3.2 - Information is organized according to a structured set of business rules and information technology requirements, which prescribe the ways in which information must be stored and handled.			

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
3.2.1	An information architecture has been defined for PCH, including information taxonomies and classification standards, as well as supporting documentation outlining the appropriate organization and structure of information	**3**	Comprehensive information architecture has not been defined for the Department. Classification standards exist for some records, for example hardcopy records utilizing iRIMs and some corporate databases.
3.2.2	Tools and guidelines have been provided to ensure information of business value can be classified according to PCH classification standards	**3**	A comprehensive suite of tools and guidance has not been provided to ensure information can be classified according to business value, although some tools exist such as iRIMs (for paper records), and some corporate databases.
4. Use and Dissemination			
4.1 - Effective use and dissemination of information yields timely, accurate and available information that is accessible by those who need it, when they need it, and in a form that they can use.			
4.1.1	IM enabling tools and systems allow for the searching and retrieving of information throughout the Department.	**3**	Given the current utilization of repositories (i.e., restricted access network drives), and the lack of a comprehensive information architecture, the ability to search and find information throughout PCH is limited. In general documents are requested and provided by email.
4.1.2	Branches/program areas have identified their information use and disclosure requirements related to their mandate, including their regulatory and reporting requirements.	**1**	For those branches/program areas with specific regulatory or legislative requirements, formal processes have been established to ensure these requirements are met.

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
4.1.3	Processes and systems are integrated to limit multiple data entry and more than one source of the same information.	**3**	The same information is often in several places and formats. For example, G&C related information such as program application forms and program correspondence is often managed through email, documents or databases on the network drives, GCIMS, and/or hardcopy files.
4.1.4	Appropriate data sharing agreements are established when information is shared with other organizations.	**3**	There has been no specific guidance or standards related to data sharing provided by KIM. In general there were few instances of data sharing identified during the audit; where data sharing with government partners and stakeholders was identified, formal agreements were not in place.
4.1.5	Access to information requests are responded to in a timely and appropriate manner.	**1**	Access to information requests are responded to in a timely and appropriate manner.
5. Maintenance, Protection and Preservation			
5.1 - Long-term availability, understandability and usability of information assets is maintained.			
5.1.1	Information repositories have sufficient controls to protect the availability, understandability and usability of information.	**2**	There are currently no specific standards related to ensuring information repositories controls for the availability, understandability and usability of the information**;** however, based on testing, information was available, understandable, and useable.
5.2 - Information privacy and security measures have been implemented based on the sensitivity of the information to ensure it is protected from unauthorized use or disclosure.			

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
5.2.1	Practices are established to ensure policies and procedures related to the privacy and security of information is consistent with the sensitivity of the information.	**3**	Standards for the security classification of information, and the appropriate safeguards to protect personal and other sensitive information, are inconsistent and/or are not being applied. In addition, PCH has not yet developed a comprehensive Privacy Management Framework for the Department to identify and mitigate privacy risks and help ensure compliance with *Privacy Act.*
5.2.2	Access controls are utilized to limit access to information on a need to know basis, for both electronic and hardcopy data.	**3**	Access controls related to hardcopy records and databases is generally well controlled, although of note i) the corporate Records Office managed by KIM has not specifically segregated records based on level of sensitivity, and ii) access controls related to the information managed in the Department network drive are difficult to maintain, given the need to manage access to different folders. In certain cases, the network folder for a branch is available to anyone within the branch.
6. Disposition			
6.1 - Information that no longer has business value are disposed of appropriately, or transferred for archiving to Library and Archives Canada.			
6.1.1	A process has been established to obtain and review record disposition authorities (RDAs) for all information holdings.	**3**	PCH holds a number of institution-specific RDAs from LAC covering its information resources collections up to the early 1990's. KIM is currently working with program areas and LAC to obtain additional RDAs. Approximately half of the 100 PCH programs/units identified by KIM as requiring institution-specific RDAs have yet to obtain a RDA.

Criteria #	Audit Criteria	Con-clusion on Audit Criteria	Examples of Key Evidence / Observation
6.1.2	Branches/regions adhere to appropriate retention and disposition schedules as outlined in the applicable RDA.	**3**	Electronic records are not being consistently disposed of, and in many cases are being retained indefinitely. Hardcopy records related to specific program activities regularly considered for disposition. Hardcopy records related to other business activities were not subject to such a formal disposition process.
7. Monitoring and Evaluation			
7.1 - A performance management process has been established, which includes monitoring compliance and assessing continuous improvement.			
7.1.1	A performance management process has been implemented, and monitoring activities have been implemented related to compliance with IM requirements	**3**	A performance management process has not been implemented, although PCH is developing a plan for the development of performance measures.

Appendix B – Definitions and Acronyms

Acronyms

ARB	Architecture Review Board
ATI	Access to Information
ATIP	Access to Information and Privacy
BOC	Business Operations Committee
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
DAC	Departmental Audit Committee
DSO	Departmental Security Officer
EAC	Enterprise Architecture Committee
EDRMS	Electronic Document and Record Management System
G&C	Grants and Contributions
GCIMS	Grants and Contributions Information Management System
GCMI	Grants and Contributions Modernization Initiative
GC	Government of Canada
IM	Information Management
iRIMs	Integrated Recorded Information Management System
KIM	Knowledge and Information Management Directorate
LAC	Library and Archives Canada
MAF	Management Accountability Framework
MIDA	Multi-Institutional Disposition Authority
PCH	Department of Canadian Heritage
PEA	Planning and Enterprise Architecture
PIA	Privacy Impact Assessment
RBAP	Risk-Based Audit Plan
RDA	Retention and Disposition Authority
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment

Definitions

Disposition	Disposition refers to the process which enables government institutions to dispose of records which no longer have operational value, either by permitting their destruction (at the discretion of institutions) or by requiring their transfer to LAC. Federal government institutions may not destroy a record without a proper RDA. RDAs may be: 1.) Multi-Institutional Disposition Authorities that relate to records managed by all or a multiple number of government institutions, and allow the institutions to dispose of records under certain terms and conditions; or 2.) Institution Specific Disposition Authorities that relate to records managed by a single government institution, and allow the institution to dispose of their records under certain terms and condition.

Security Classification of Information	The *Policy on Government Security* requires federal government organizations to implement appropriate safeguards based on the sensitivity of the information that they manage. Furthermore, the Directive on Departmental Security Management, further expands on this requirement, indication that organizations must identify and categorize information based on the degree of injury that could be expected to result from the compromise of its confidentiality, with confidentiality defined as the "*characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests*." **'**Classified information', refers to information that, if inappropriately disclosed, would *cause injury to national interests.* Classified information can be determined to be *Top Secret*, *Secret* or *Confidential*, based on the level of injury that would be caused by the unauthorized disclosure of the information. 'Protected information' refers to personal or business confidential information as it relates to information that, if inappropriately disclosed, would *cause injury to private and other non-national interests* (e.g. to an individual). the confidentiality of protected information is ranked from *Protected A* (low confidentiality requirements) to *Protected C* (high confidentiality requirements), and is assessed based on the potential for disclosure of the information to unauthorized individuals to cause harm to personal and other non-national interests.
Directive on Recordkeeping	Recordkeeping in the TBS *Policy on Information Management* is defined as: **"***A framework of accountability and stewardship in which records are created, captured, and managed as a vital business asset and knowledge resource to support effective decision making and achieve results for Canadians."* The TBS *Directive on Recordkeeping* came into effect on June 1, 2009. The Directive states that TBS will review its effectiveness within five years of its publication date – June 2009. Institutions, therefore, have until Spring 2014 to implement it. Compliance will be measured through MAF. The TBS *Directive on Recordkeeping* specifies five (5) requirements to be met by institutions. • Identification of Information Resources of Business Value; • Protection of Information Resources of Business Value; • Life Cycle Management of Information Resources of Business Value; • Documentation of Information Resources of Business Value; and • Training and Awareness.

Appendix C: Management Action Plan

Response to Information and Records Management Audit

Chief Information Management Branch (CIOB)
Knowledge and Information Management Directorate (KIM)
October 2011

This document represents the Management Action Plan response to the Information and Records Management Audit conducted by PCH Audit and Assurance Services Directorate. The response is arranged in order of the following themes:

A. Foundation Building – Section 5.1, 5.2 and Section 5.3

These sections relate to the IM Strategy, IM Outreach/Training - IM Roles and Responsibilities and to IM Standards, Practices and Tools, all of which are key components regarding IM and Recordkeeping functions. The activities described in this section demonstrate how CIOB plans to address this topic within the audit report. The outcome of these activities will be more knowledgeable and aware employees and will facilitate information of business value being considered as a strategic resource in service of improved decision-making.

B. Improved Recordkeeping – Section 5.3 and Section 5.4

This section relates to IM Standards, Practices, and Tools and to Retention and Disposition Practices, both of which involve improvements to Recordkeeping at PCH. The activities described in this section demonstrate how CIOB plans to address this topic within the audit report. It further demonstrates the commitment of the CIO to work with Library and Archives Canada (LAC) to address the finding of the audit report relating to this topic. These activities will enable the consistent and standardized approach to information resources that will improve the finding of corporate information. Finding information resources of business value more easily will help deliver PCH programs and services more efficiently and ultimately improve service to Canadians.

C. Partnerships / Engagement – Section 5.2 and Section 5.5

These sections relate to IM Outreach/Training - IM Roles and Responsibilities and the Protection of Sensitive Information, both of which involve collaboration with IM stakeholders within PCH and the GC community. The joint activities described in this section demonstrate the level of engagement that will be undertaken by CIOB to address the opportunities cited within the audit findings. These activities will increase the spirit of collaboration and within PCH and the GC community. It is well known that increased collaboration yields more productivity in the workplace. The activities relating to protection of sensitive information will also enable information resources to be protected as strategic assets as expressed in the Departmental PAA.

Management Action Plan			
5.1 IM Strategy (Foundation Building)			
Recommendation	**Actions**	**Who**	**Target Date**
The Chief Information Officer (CIO) should: **1.1.** Actively engage the Department's **governance committees** for input into the current draft IM Strategy, and considering available resources, specifically prioritize objectives/ initiatives, including a **performance measurement plan**, with a consideration of the **risks** to the Department of not achieving specific objectives in the Strategy.	**Agree.** *1.1.1* **Governance Committees**: *a.)* Present IM Strategy draft (for 2012-17), which will include strategic goals, priority initiatives, associated risks and resource requirements to IM/IT Enterprise Architecture Committee (Level 4) for feedback / direction / endorsement.	*1.1.1a.)* Director, KIM	*1.1.1a.)* Q4 2011/12
	b.) Present IM Strategy to Level 3 Governance and above for approval, incorporating feedback received from Level 4.	*1.1.1b.)* CIO / Director, KIM	*1.1.1b.)* Q4 2011/12
	Agree. *1.1.2*. **Performance Measurement Plan**: *a.)* An Implementation Plan will accompany the IM Strategy and include performance measures.	*1.1.2a.)* Director, KIM - IM Strategic Policy and Planning	*1.1.2a.)* Q3 2011/12
	b.) Elaboration of full Departmental Performance Measurement Framework for Information Management (IM) as part of Phase 3 of Departmental IM Policy implementation. This initiative is undertaken in a phased approach	*1.1.2b.)* Director, KIM - IM Strategic Policy and Planning	*1.1.2b.)* Elaboration will be carried out in phases - Q3 2011to Q2 2014

	outlined in the *IM Policy Implementation Plan*.		
	Agree. *1.1.3.* **Risk:** A Risk Assessment will be included in the draft IM Strategy.	*1.1.3.* Director, KIM - IM Strategic Policy and Planning	*1.1.3.* Q3 2011/12
5.2 IM outreach/training and IM roles/responsibilities (Foundation Building / Partnerships and Engagement)			
Recommendation	**Actions**	**Who**	**Target Date**
In setting priorities in the IM Strategy, the CIO should consider: **2.1.** Engaging with branches/regions to define current IM capabilities and capacity within the branches/regions, and enabling further collaboration to ensure these IM resources can be effectively utilized. Activities should be intended to help position the Department to further standardize IM resource roles.	**Agree.** *2.1.* **Define IM capabilities and capacity within branches/regions and standardize IM resource roles:** *a.)* Leverage IM Community of Practice to continue to provide guidance on role of IM specialists, to pursue new departmental collaborative IM initiatives and to explore technology options for more effectively including regional IM representatives.	*2.1a.)* Director, KIM - IM Client Services	*2.1a.)* Q4 2011/12
	b.) Expand methods used to communicate PCH managers' IM roles and responsibilities - in collaboration with HR (Managing @PCH and Working @PCH orientation presentations to new employees and new managers) and through leveraging the IM Intranet Site Guidance page.	*2.1b.)* Director, KIM – IM Policy and Planning	*2.1b.)* Q3 2011/12 and ongoing

	c.) Study options for the creation of IM Specialist positions within the Sector Hubs structure and define potential roles and responsibilities.	*2.1c.)* Director, KIM – IM Client Services	*2.1c.)* Q4 2011/12
	d.) Raise awareness of all employees' IM roles and responsibilities through awareness sessions including presentations of IM Basics as part of the KCS Knowledge Exchange Series and via other forums.	*2.1d.)* Director, KIM – IM Strategic Policy and Planning	*2.1d.)* Q3 2011/12 and ongoing
	e.) Investigate provision of mandatory annual IM awareness sessions on a rotational basis to all branches and all new employees (similar to annual DSO briefings).	*2.1e.)* Director, KIM – IM Policy and Planning	*2.1e.)* Q3 2011/12 and ongoing
	f.) Conduct an organizational review of how IM is structured and delivered across PCH regional offices with a view toward greater standardization and consistency. The use of pressure funding will likely be required for this activity.	*2.1f.)* CIO / Director, KIM	*2.1f.)* 2012/13
	g.) Develop a comprehensive suite of IM-related standards and tools to support the PCH IM Policy (an IM Policy Suite), to provide IM guidance and introduce consistency in IM practice. This initiative is underway with working group participation from all sectors, including Regions, in the formulation and review. Pressure	*2.1g.)* Director, KIM - IM Strategic Policy and Planning	*2.1g.)* Q4 2011/12 – 2012/13

	funding will be used to provide a primary set of Policy Suite documents. Additional pressure funding will be required for development of future sets of secondary and tertiary priority level documents.		
	h.) Continue to participate in and leverage TBS and/or departmental initiatives regarding generic approaches to IM organizational models and work descriptions with a view toward standardization.	*2.1h.)* Director, KIM - IM Strategic Policy and Planning	*2.1h.)* 2011/12 and ongoing
Recommendation	**Actions**	**Who**	**Target Date**
In setting priorities in the IM Strategy, the CIO should consider: **2.2.** Ensuring the KIM further collaborates with the Access to Information Privacy (ATIP) Secretariat and Departmental Security to establish formal mechanisms for considering IM requirements during the assessment and development of privacy and security controls throughout PCH.	**Agree.** **Establish formal mechanisms regarding IM requirements during the assessment and development of privacy and security controls:** *a.)* Continue collaboration regarding the incorporation of IM requirements in developing privacy and security controls which form part of the IM/IT Project Review.	*2.2a.)* Director(s), KIM/ATIP/DSO/IT Security/CIOB Architecture Review Board (ARB) / Enterprise Architecture Committee (EAC)	*2.2a.)* 2011/12 and ongoing

	b.) Ensure that the corporate IM group is informed of Privacy Impact Assessments (PIA) and Threat Risks Assessments (TRA) assessments and their results.	*2.2b.)* Director(s), IT Security/ATIP and DSO	*2.2b.)* Q3 2011/12 and ongoing
	c.) Increase availability of Departmental Security Officer (DSO) tools and continue consultation with IM/ IT clients.	*2.2c.)* DSO	*2.2c.)* Q4 2011/12 and ongoing
	d.) Ensure that ATIP, DSO and IT Security continue to be represented at Business Operations Committee (BOC).	*2.2d.)* CIO	*2.2d.)* Q4 2011/12 and ongoing
5.3 IM Standards, Practices, and Tools (Foundation Building / Improved Recordkeeping)			

Recommendation	Actions	Who	Target Date
In setting priorities in the IM Strategy, the CIO should consider: **3.1.** Prioritizing the completion of the information architecture for the Department, with an initial focus on the classification of records throughout the Department, regardless of format or medium.	**Agree.** *3.1.* **Information architecture for PCH, with initial focus on classification of records:** *a.)* Develop a new information architecture / classification scheme for PCH. This information architecture will include considerations related to the security classification of information. This is a project already funded through pressure funding, underway and will require additional pressure funding to complete. This will be a cornerstone of departmental enterprise architecture and a priority pre-requisite for EDRMS deployment.	*3.1a.)* Director, KIM - IM Client Services in collaboration with Planning and Enterprise Architecture (PEA)	*3.1a.)* 2011-2013
	b.) In the context of development of a new classification scheme, ensure that the emerging IM Policy Suite includes required classification standards and procedures.	*3.1b.)* Director, KIM - IM Strategic Policy and Planning	*3.1b.)* 2011 - 2013
5.4 Retention and Disposition Practices (Improved Recordkeeping)			
Recommendation	**Actions**	**Who**	**Target Date**
In setting priorities in the IM Strategy, the CIO should consider: **4.1.** Determining the extent to which more generic Record Disposition Authorities (RDAs) can be utilized for program	**Agree and CIO will take direction from LAC regarding generic RDAs.** *4.1.* **Generic RDAs:** *a.)* In the context of the Library and	*4.1a.)* LAC in collaboration with Director, KIM – IM	*4.1a.)* Dependent on availability of LAC generic

areas that currently do not have an approved RDA, in order to reduce the number of RDAs for which approval is required. The process standardization work of the GCMI could be leveraged in this context.	Archives Canada (LAC) Recordkeeping Methodology, LAC will perform assessments of all departments that will, in part, determine generic and specific RDAs.	Client Services	RDAs for programs (LAC is aiming for Q3 2011/12)
	b.) The new classification scheme will regroup similar departmental functions, thereby facilitating the creation by LAC of generic RDAs for PCH.	*4.1b.)* Director, KIM – IM Client Services	*4.1b.)* Q2 2012-13
In setting priorities in the IM Strategy, the CIO should consider: **4.2.** Assisting program areas in identifying information that is no longer of business value. This should include the development of strategies in collaboration with program areas on the disposition of information that is stored in electronic databases.	**Agree.** *4.2.* **Identifying information no longer of business value:** *a.)* IM Awareness Days, IM Basics presentations, and the new Departmental IM Handbook will disseminate knowledge of what to keep /delete.	*4.2a.)* Director, KIM – IM Policy and Planning	*4.2a.)* Q3 2011/12 and ongoing
	b.) Create a Task Team for EDRMS pre-deployment readiness phase activities such as shared drive clean-up; identifying and inventorying information resources of business value (records); consolidation of repositories; clarification of retention and disposition periods; implementation of new classification structure. The creation of a Task Team will need to be funded through pressure	*4.2b.)* Director, KIM - IM Client Services	*4.2b.)* 2012-2014

	funding.		
5.5 Protection of Sensitive Information (Partnerships and Engagement)			
Recommendation	**Actions**	**Who**	**Target Date**
In setting priorities in the IM Strategy, the CIO, in collaboration with the Departmental Security Officer and the ATIP Coordinator, should consider: **5.1.** Ensuring that the development of the information architecture for the Department includes considerations related to the security classification of information, as well as ensuring there are appropriate safeguards implemented, and tools available, for the management of classified information. This includes conducting Threat and Risk Assessments (TRAs), for example on the corporate Records Office, and Privacy Impact Assessments (PIAs), for example, on the PeopleSoft upgrade.	**Agree and will work with DSO to determine appropriate measures regarding physical space such as Corporate Records Office.** *5.1.* **Security:** *a.)* Conduct TRAs and PIAs on the EDRM solution and any other information-focused corporate system initiative. This requirement is already part of the ongoing IM/IT project process.	*5.1a.)* Director, KIM / EDRMS Project Team	*5.1a.)* Q4 2011/12 and ongoing
	b.) Maintain the objective of implementing a Protected B EDRMS environment. This will be dependent on the eventual configuration of the Shared Services Canada GCDOCS EDRMS solution.	*5.1b.)* Director, KIM - EDRMS Project Team / Shared Services Canada	*5.1b.)* 2012- 2014

	c.) Ensure that metadata intended to capture security classification of information objects is introduced into the new classification scheme and assessed during proof of concept and piloting.	*5.1c.)* Director, KIM – Client Services	*5.1c.)* Q4 2011/12
	d.) The appropriate safeguards and assessments will be done.	*5.1d.)* Part of the ongoing IM/IT project review process	*5.1d.)* 2011/12 and ongoing
	e.) The appropriate safeguards and assessments will be done.	*5.1e.)* Director, Facilities Management and DSO	*5.1e.)* 2011/12 and ongoing
	f.) Provide guidance and any assistance/advice required to ensure proper privacy protocols/controls are followed and any PIAs are initiated as required.	*5.1f.)* Directors, KIM and ATIP	5.1f.) 2011/12 and ongoing
	g.) Promote use of the online Information Classification Guide; Identity Management Directive; Entrust software; physical security consultations; and security awareness sessions.	*5.1g.)* Director(s) KIM/ATIP and DSO	*5.1g.)* 2011/12 and ongoing
	h.) Promote use of secure equipment (access control; secure filing cabinets and filing rooms; secure faxes and phones; shredders).	*5.1h.)* DSO	*5.1h.)* Q4 2011/12 and ongoing

	i.) Increase physical security sweeps as per Security Sweep PCH Policy which flows from the Government of Canada Security Policy.	*5.1i.)* DSO	*5.1i.)* 2011/12 and ongoing
In setting priorities in the IM Strategy, the CIO, in collaboration with the Departmental Security Officer and the ATIP Coordinator, should consider: **5.2.** Ensuring additional training and awareness on the security classification of information is provided to staff, focused on appropriate safeguards based on the level of sensitivity of the information being managed.	**Agree.** *5.2.* **Training and awareness on the security classification of information:** *a.)* With the objective of a comprehensive approach, expand IM Awareness events such as "IM Awareness Days" and related initiatives to include the DSO and IT Security. These events already include ATIP.	*5.2a.)* Director, KIM – IM Strategic Policy and Planning / ATIP / DSO / IT Security	*5.2a.)* 2012/ 13 and ongoing
	b.) Provide mandatory annual awareness sessions on security awareness on a rotational basis to all branches and to all new employees.	*5.2b.)* DSO	*5.2b)* 2011/12 and ongoing
	c.) Ensure that security consultations are available	*5.2c.)* DSO	*5.2c.)* 2011/12 and ongoing
	d.) Continue "Security Awareness" booth and emails focusing on safeguarding information	*5.2d.)* DSO	*5.2d.)* 2011/12 and ongoing