PARKS CANADA AGENCY

AUDIT OF INFORMATION MANAGEMENT

Prepared by:
Deloitte & Touche LLP

Final Report

July 2009

Catalogue No. : R64-369-2010E-PDF
ISBN : 978-1-100-15085-7

TABLE OF CONTENTS

Report submitted to the Parks Canada Audit Committee on September 10th, 2009.

EXECUTIVE SUMMARY

This Information Management (IM) audit assesses the adequacy and effectiveness of Parks Canada's (PCA) current IM Control Framework, and the extent to which it supports the Agency's ability to be in compliance with the IM-related requirements of the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act*, as well as related Treasury Board policy requirements. These requirements are outlined in Appendix A. The Agency's IM management control framework should support the appropriate management of information through each of the seven (7) steps in the Records and Information Life Cycle.

PCA operations are decentralized throughout the country. National office consists of six directorates (National Parks, National Historic Sites, Strategy and Plans, Human Resources, Infrastructure and Real Property, and External Relations and Visitor Experience) that provide legislative, operational policy, planning, program direction, financial management, and human resources functions and services. Program delivery is the responsibility of PCA's 32 field units, which consist of groupings of national parks, national historic sites and national marine conservation areas. The work of field units is supported by regional service centres. To ensure appropriate audit coverage and a representative sample, audit work was conducted at national office, as well as within selected service centres and field units.

A risk-based audit program was developed through a preliminary risk assessment process, which included interviews and a review of documentation from a cross-section of PCA national office, service centre and field unit areas. As part of the audit program, audit criteria, legislative and policy requirements related to the audit criteria, control activities, and audit procedures were developed. The conduct of the audit itself included additional interviews and documentation review, and to the extent IM controls existed, these were tested. At the end of the audit, a debrief meeting was held with the Chief Information Officer and the Chief Administrative Officer to discuss and validate the findings and recommendations contained in the report.

The audit was conducted in accordance with the standards set out in the Treasury Board (TB) Policy on Internal Audit. These standards require that the audit is planned and performed in a manner that allows the audit team to determine assurance of the audit findings. Sufficient audit work has been performed and the necessary evidence has been gathered to support the conclusions contained in this report. The audit was conducted between February 2009 and June 2009.

The audit's observations and recommendations have been made in accordance with the PCA Audit Reporting Rating System described below:

Audit Reporting Rating System		
RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.
YELLOW	Moderate Improvements Needed	Some controls are in place and functioning. However, major issues were noted and need to be addressed. These issues could impact on the achievement or not of program/operational objectives.
BLUE	Minor Improvements Needed	Many of the controls are functioning as intended. However, some minor changes are necessary to make the control environment more effective and efficient.
GREEN	Controlled	Controls are functioning as intended and no additional actions are necessary at this time.

The audit has identified that PCA's current IM management control framework is weak, with significant improvements required (a rating of 'orange'). Based on PCA's current IM management control framework, there is a significant risk that PCA is not compliant with IM legislative and policy requirements.

IM Management Control Framework		
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

The audit also specifically assessed how the IM management control framework supports compliance with the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act*.

The audit determined controls related to compliance with the *Access to Information Act* were weak, with significant improvements required (a rating of 'orange').

Access to Information Act		
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

The audit determined controls related to compliance with the *Privacy Act* were not functioning, with immediate action required (a rating of 'red').

Privacy Act		
RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

The audit determined controls related to compliance with the *Library and Archives of Canada Act* required moderate improvements (a rating of 'yellow').

Library and Archives of Canada Act		
YELLOW	Moderate Improvements Needed	Some controls are in place and functioning. However, major issues were noted and need to be addressed. These issues could impact on the achievement or not of program/operational objectives.

The table below outlines the rating provided to PCA for the effectiveness of each audit criterion. A conclusion on the effectiveness of each audit criterion and recommendations to address the audit findings for each criterion is provided in Appendix A. A full list of recommendations is provided below the table.

Audit Criteria	Rating
1. Information Management Planning	
1.A. An IM plan and strategy has been developed and implemented. Resources are sufficient based on the plan and strategy, and IM staff have the appropriate experience and skills.	Orange - Significant Improvements Needed
1.B. An IM governance and accountability framework has been implemented, including defined roles and responsibilities.	Orange - Significant Improvements Needed
1.C. Training and awareness initiatives related to IM have been implemented	Orange - Significant Improvements Needed
1.D. Appropriate IM policies and procedures apply to national, service centre and field unit levels and have been appropriately communicated.	Orange - Significant Improvements Needed
***2.* Collection, Creation, Receipt and Capture**	
2.A. The information collected supports PCA objectives and legislative/program requirements	Yellow - Moderate Improvements Needed
2.B. Formal procedures and guidelines have been developed to ensure information is assessed at time of creation related to its role and business value	Orange - Significant Improvements Needed
3. Organization of Information	
3.A. Recordkeeping repositories have been designated to maintain information resources of business value	Red - Unsatisfactory
3.B. Records and information are organized according to a structured set of business rules and information technology requirements, which prescribe the ways in which records and information must be stored and handled.	Orange - Significant Improvements Needed
4. Use and Dissemination	
4.A. Effective use and dissemination of records and 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. Appropriate controls have been implemented related to access to information requests and the sharing of information with third parties.	Orange - Significant Improvements Needed
5. Maintenance, Protection and Preservation	
5.A. Long-term availability, understandability and usability of information assets is maintained	Orange - Significant Improvements Needed
5.B. Appropriate data privacy and security measures have been implemented based on the sensitivity of the data	Red - Unsatisfactory
6. Disposition	
6.A. Records are disposed of that no longer have business value or transferred for archiving to Library and Archives Canada	Red - Unsatisfactory
7. Evaluation/Monitoring	
7.A. Process established to report performance, which includes monitoring compliance and assessing continuous improvement.	Red - Unsatisfactory

Based on the findings of the audit, the following recommendations have been provided. These recommendations are also linked to the appropriate criterion and associated legislative and policy requirements in Sections 6.1 of the report. Failure to implement these recommendations will limit PCA's ability to meet legislative requirements. Of note, recommendations may address issues within multiple criteria. These recommendations are addressed to the Chief Information Officer:

[1] Ensure IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. Within regions, ensure the service centre business plan also considers IM requirements, and that these are incorporated into the yearly planning process conducted between service centres and the field units.

[2] Review the long-term purpose and role of the record centres and determine their resource requirements.

[3] Develop an IM governance and accountability framework. This includes implementing an IM oversight committee and establishing a formal mechanism, led by national office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels.

[4] Develop an IM training strategy that considers IM training needs based on priority levels (e.g. Senior Managers involved in strategic decision making, IM Officers), and enhancements required to the online course and other learning/awareness channels. This includes appropriate and specific training and resource material provided to IM staff to help them meet the requirements of their job descriptions. Track attendance to IM training as required.

[5] Ensure national systems can respond to regional needs and these national systems are being fully utilized.

Review current use of databases at the service centre and field unit level and identify opportunities for these to be eliminated and replaced with existing national systems that offer the same functionality.

Ensure priority is placed on those activities that have the highest requirements for the business value, confidentiality, integrity and availability of information.

To the extent 'local' databases may need to be developed, develop guidance and a checklist related to the development of databases that outline IM and other considerations (i.e., determining business requirements and assessing appropriate security and privacy controls).

[6] Create a central forms unit responsible for the creation and management of information collection forms. Only forms developed and approved by this unit should be authorized to be used within PCA. The form unit should ensure forms adhere to legislative and policy requirements, and forms used to collect personal information are reviewed by ATIP.

[7] Develop an information asset inventory that captures the key information and its business value and role within PCA, including personal information in order to update PCA's current Personal Information Banks (PIBs) in InfoSource. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their information collection needs and the role and business value of the information collected.

[8] Develop an information classification standard to ensure the consistent organization of hardcopy and electronic information.

[9] Implement an integrated electronic document and record management (EDRM) suite that includes a single point of access to all relevant electronic documents and structured data repositories.

[10] Ensure Memoranda of Understanding (MOU) are established for all activities involving data sharing with third parties. Develop a process to ensure appropriate approval and oversight is provided for all data sharing activities.

[11] Ensure consistent IM protocols are established prior to the collection of information for activities such as monitoring programs.

[12] Develop IT backup policies and procedures, which should be incorporated as part of a formal business continuity management and disaster recovery plan. As part of this process, review the environmental controls of records centres and server rooms, and identify essential records.

[13] Based on Policy requirements, conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) on national systems, with a priority placed on those systems containing the most sensitive information. Develop a privacy and security risk assessment policy defining when to conduct a PIA/TRA and a formal process for the completion and approval of PIAs/TRAs.

[14] Use the existing ATIP work plan to create a risk-based management framework that considers the structures, policies, systems and procedures to distribute responsibilities, coordinate work, manage risks and ensure compliance with the *Privacy Act* and *Access to Information Act.* Dedicate the necessary resources to ensure the current backlog of access to information requests is addressed.

[15] Ensure a Records Disposition Authority is approved by Library and Archives Canada. In the interim, provide further guidance on the use of the Multi-Institutional Disposition Authority (MIDA).

[16] Ensure that a policy and process for IM-related breaches and incidents is implemented, including their appropriate tracking and follow-up.

Overall Management Response

In the Fourteenth Annual Report to the Prime Minister on the Public Service of Canada, the Clerk stated that we are all faced with high public expectations for "speedy decisions, immediate responses from government, transparency in government operations, and public engagement in decision making". As a result, the Treasury Board continues to introduce more structure via frameworks, policies, directives and assessments such as the Management Accountability Framework, revised policy instruments on Information Management, Information Technology, Security, and Access to Information, Privacy Impact Assessments, and Directive on Recordkeeping. However, the Treasury Board has not funded the adoption and implementation of these new structures.

In keeping with its' mandate, Parks Canada's focus has been on service to the public and to the diverse communities where parks and historic sites are located. At times, service to the public, within limited budgets, has taken precedence over, and diverted attention from, effective information management.

Governance is a critical success factor in a geographically dispersed organization like Parks Canada, and until recently, Parks Canada has not had an Agency-level process and committee to effectively govern Information Management. With the creation of the Parks Canada Enterprise Information Committee (first meeting was held in September 2009), increased emphasis will be placed on information management, functional guidance, procedures, tools and support.

Moreover, in this information age, it is expected that all its information sources should be fully integrated and accessible, any time anywhere from any communication device. Currently, the Agency does not have the necessary information systems, procedures, tools, storage for information handling and records management to support decision-making and Agency Obligations related to Government of Canada Acts, Policies and legislations. This creates risks related to privacy, duplication and discovery of information. For these reasons, the Agency will be producing a comprehensive tactical plan that will:

- address information management as a priority;
- implement improved an information management and recordkeeping discipline; and,
- integrate collaboration, content and records management systems with information systems and technology support to improve access to the Agency's information resources (e.g. information , data, and textual records and documents).

In conclusion, Information Management and managing information are critical to achieving the PCA mandate. With leadership and ongoing support from senior managers and employees, the Agency will fulfill its Information Management obligations for preserving a record of its business, operations and activities and meeting demands for sharing its knowledge. Transformation of the Information Management program will be a critical contributor to the Agency's long-term prosperity.

1. BACKGROUND

Parks Canada Agency (PCA) is conducting audits of field units, service centres and the national office to review key financial, administrative and management practices. The audits focus on compliance with Treasury Board Secretariat (TBS) and PCA policies and practices. This audit of Information Management (IM) was conducted as part of this initiative.

No formal internal audit had been conducted previously on the IM function at PCA, but the completion in March 2009 of a description and preliminary survey of the Information Technology (IT) universe identified the IM environment as a high-risk area. The Corporate Risk Profile for 2009-10 also identified IM as a corporate risk. Failure to capture and manage pertinent data and information may hinder PCA's ability to effectively manage its operations and meet program activity architecture (PAA) objectives, as well as its legal requirements. PCA must comply with the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act*, as well as related Treasury Board policy requirements. PCA must also comply with the IM requirements of other specific legislation including the *Parks Canada Agency Act, Species at Risk Act, Canada National Parks Act, Canada National Marine Conservation Areas Act,* and *Historic Sites and Monuments Act.*

The Agency must demonstrate that its IM management control framework supports the appropriate management of information through each of the seven (7) steps in the Records and Information Life Cycle[1].

2. OBJECTIVES AND SCOPE

The objectives of this audit were to determine whether due diligence is being exercised in the key management processes for IM and to ensure to senior management that processes and controls are in place to limit risks of non-compliance with TBS and PCA policies with specific emphasis on the extent to which the current IM framework supports the Agency's ability to be in compliance with the IM-related requirements of the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act*.

The audit cannot ascertain PCA's compliance with IM-related statutory requirements, as this would require prohibitive 100% testing of all collections, uses and disclosures of information. Instead, the audit has assessed the extent to which the current IM management control framework supports PCA's ability to be in compliance with these statutory requirements.

[1] For further information refer to Libraries and Archives Canada, specifically www.collectionscanada.gc.ca/government/products-services/007002-2012-e.html

3. METHODOLOGY

Audit criteria have been categorized using the seven (7) steps in the Records and Information Life Cycle[2] and based on Government of Canada (GC) IM legislative and policy requirements. IM legislative and policy requirements that were considered included:

- *Privacy Act;*
- *Library and Archives of Canada Act;*
- *Access to Information Act;*
- Policy on Information Management;
- Directive on Information Management Roles and Responsibilities;
- Policy on Privacy Protection;
- Access to Information Policy; and,
- Government Security Policy.

Of note, the draft Directive on Recordkeeping from Library and Archives of Canada was also considered during the development of recommendations to assist PCA in aligning with the new requirements contained in the Directive.

A risk-based audit program was developed through a preliminary risk assessment process, which included interviews and a review of documentation from a cross-section of PCA. As part of the audit program, audit criteria, control activities, and audit procedures were developed, and legislative and policy requirements were mapped to each audit criteria (refer to Appendix A). The conduct of the audit itself included additional interviews and documentation review, and to the extent IM controls existed, these were tested utilizing further audit procedures. At the end of the audit, a debrief meeting was held with the Chief Information Officer and the Chief Administrative Officer to discuss and validate the findings and recommendations contained in the report.

PCA is decentralized throughout the country. Program delivery is the responsibility of PCA's 32 field units, which consist of groupings of national parks, national historic sites and national marine conservative areas. About 80% of PCA's work force is based in the field where most of its program expenditures take place. The work of field units is supported by regional service centres. To ensure appropriate audit coverage and a representative sample, audit work with service centres and field units was conducted in both the East and in the West. Separate Director General's for Eastern and Western/Northern Canada provide day-to-day oversight of field unit operations, although Superintendents of Field Units have a direct accountability to the PCA Chief Executive Officer through business plan. Audit work was also conducted at PCA national office. Site visits and audit procedures were conducted at:

- Atlantic Region Service Centre (Halifax);

[2] For further information refer to Libraries and Archives Canada, specifically www.collectionscanada.gc.ca/government/products-services/007002-2012-e.html

- Mainland Nova Scotia Field Unit (Citadel National Historic Site and Kejimkujik National Park of Canada);
- Western and Northern Service Centre (Calgary and Winnipeg);
- Banff National Park Field Unit;
- National Parks Directorate (National Office); and,
- Finance (National Office).

The audit's observations and recommendations have been made in accordance with the PCA Audit Reporting Rating System described below:

Audit Reporting Rating System		
RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.
YELLOW	Moderate Improvements Needed	Some controls are in place and functioning. However, major issues were noted and need to be addressed. These issues could impact on the achievement or not of program/operational objectives.
BLUE	Minor Improvements Needed	Many of the controls are functioning as intended. However, some minor changes are necessary to make the control environment more effective and efficient.
GREEN	Controlled	Controls are functioning as intended and no additional actions are necessary at this time.

4. ASSURANCE STATEMENT

The audit was conducted in accordance with the standards set out in the Treasury Board (TB) Policy on Internal Audit. These standards require that the audit is planned and performed in a manner that allows the audit team to determine assurance of the audit findings.

Sufficient audit work has been performed and the necessary evidence has been gathered to support the conclusions contained in this report. The audit was conducted between February 2009 and June 2009.

5. CONCLUSION

The audit has identified that PCA's current IM management control framework as weak, with significant improvements required (a rating of 'orange'). Based on PCA's current IM management control framework, there is a significant risk that PCA is not compliant with IM legislative and policy requirements, and that current IM practices do not sufficiently support PCA in meeting its program activity architecture (PAA) objectives.

IM Management Control Framework		
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

The audit also specifically assessed how the IM management control framework supports compliance with the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act*.

The audit determined controls related to compliance with the *Access to Information Act* were weak, with significant improvements required (a rating of 'orange').

Access to Information Act		
ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

The audit determined controls related to compliance with the *Privacy Act* were not functioning, with immediate action required (a rating of 'red').

Privacy Act		
RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

The audit determined controls related to compliance with the *Library and Archives of Canada Act* required moderate improvements (a rating of 'yellow').

Library and Archives of Canada Act		
YELLOW	Moderate Improvements Needed	Some controls are in place and functioning. However, major issues were noted and need to be addressed. These issues could impact on the achievement or not of program/operational objectives.

A conclusion on the effectiveness of each audit criterion is provided in Section 6.

6. OBSERVATIONS AND RECOMMENDATIONS

6.1. Parks Canada IM Management Control Framework

The following observations and recommendations are organized by the seven (7) steps in the Records and Information Life Cycle. Evaluation of PCA's IM management control framework can be ascertained by the extent it supports the appropriate management of information through each of the steps and promote compliance with the IM-related requirements of the *Access to Information Act*, the *Privacy Act* and the *Library and Archives of Canada Act.*

6.1.1 Information Management Planning

6.1.1.A Criteria

An IM plan and strategy has been developed and implemented. Resources are sufficient based on the plan and strategy, and IM staff have the appropriate experience and skills.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

At a national level, a draft of a three year IM/IT Business Plan has been developed; the business plan indicates business cases will be developed to "*clearly articulate the needs, costs and resources for the IM/IT investments".* These business cases have yet to be developed.

A longer term seven year Information Management, Systems and Technology (IMST) Strategy have been developed and approved by the Executive Board on October 14, 2008. The strategy has provided a framework related to the necessary components of an IM strategy, and outlines current and future initiatives. The strategy does not map specific IM requirements to these initiatives. The Board determined that priority was to be placed on the development of business cases: 1) to manage PCA information so that PCA can fulfill its obligations; and, 2) to define the PCA information requirements. These business cases have yet to be developed.

An Access to Information and Privacy (ATIP) Action Plan has also been developed by the PCA ATIP Coordinator in order to begin addressing the lack of focus on privacy over the last several years. From 2005-2008, Environment Canada provided ATIP support to PCA. The Action Plan includes initiatives to address PCA's access to information and privacy requirements, although the plan does not contemplate required resources or prioritize the actions based on potential risk.

At the service centre level, there is a five year rolling business plan completed jointly for all service centres. The plan was last updated in December 2007, as a decision was reached to not update the plan last year. The business plan does not explicitly address any IM-related actions or strategies. The service centres indicated they look to the national office for IM strategy, and further indicated there has been little communication from the national office in recent years. A lack of centralized direction results in inconsistent and/or inappropriate IM practices.

In general, field units have not requested specific assistance related to any IM initiatives, and the service centres have indicated they would not have the capacity to provide additional services to the field units. From a record centre perspective within the service centres, those responsible indicated that they do not have sufficient resources if all staff attempted to utilize the records centres. Maintenance at current levels has also been difficult; as an example, a records centre at one service centre had over 500 boxes of records that have yet to be inventoried or classified.

The job description for IM Officers within service centres outlines various IM activities related to being an expert resource for their region; however, some of these IM Officers are solely conducting library activities and do not possess the experience and training required to conduct all of the activities expected of IM Officers.

Conclusion

A high level plan and strategy related to IM have been developed, although the business cases outlining specific IM requirements and how they will be met, as well as required resources, have not been developed. Many IM Officers have retained their librarian roles and do not possess the appropriate experience and training to fulfill the expectations outlined within the job descriptions for IM Officers.

Recommendations

[1] The Chief Information Officer should ensure IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. Within regions, ensure the service centre business plan also considers IM requirements, and that these are incorporated into the yearly planning process conducted between service centres and the field units.

Management response:

AGREE.

1.1 The Agency has committed to a new Governance structure for Information Management, Systems and Technology, led by the Enterprise Information Committee (EIC). Its' main responsibilities include reviewing all proposed and, on a prioritized basis, on-going projects/initiatives to ensure that IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. To ensure Agency-Wide IM requirements are incorporated into IM planning and effective integration of Field unit and service centre and national office IM planning, EIC Membership includes DG East (chair), CFO (Internal Services including

Financial Management) and there is a member from each Program Activity, and members from Service Centres and Field Units (East and Western and Northern). **Target date: October 2009**.

1.2 A strategic plan for PCA IM, IS and IT (IMST Strategic Plan) will be developed and presented to EIC identifying current plans for IM, IS, and IT given current resource levels, as well as options, with associated costs, for providing a sustainable Service for IM. With EIC endorsement, the tactical plan and options will be provided to Finance Committee for consideration/approval. **Target date: June 2010.**

1.3 National Directorates, Service Centre and Field Unit business plans will be reviewed to ensure that IM requirements are incorporated into yearly planning process including business continuity planning conducted between the Service Centres and the Field Units. **Target date: December 2010.**

> **[2]** The Chief Information Officer should review the long-term purpose and role of the record centres and determine their resource requirements.

Management response:

AGREE

Parks Canada will negotiate with Canadian Heritage for a cost effective extension (2010-2011) to the existing Memorandum of Understanding for PCH to continue to provide the paper based storage for National Office information holdings; library services in National Office; and, ongoing provision of information systems for the records management system for legacy paper based records and library catalogue**. Target date: June 2010.**

Parks Canada will assess the long-term role of the record centres when defining the IM Service Model. The resource requirements for managing records will be defined in the Parks Canada Records Strategy. The assessment of records centres (e.g. National Office Directorates, Regional Service Centres, and Field Units, Library and Archives Canada) will be included in the environmental and organizational scan of existing services and assets. **Target date: December 2010.**

> **[3]** The Chief Information Officer should develop an IM governance and accountability framework. This includes implementing an IM oversight committee and establishing a formal mechanism, led by national office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels.

Management response:

AGREE.

3.1 The Executive Board approved the creation of the Enterprise Information Committee (EIC). The inaugural meeting will occur on September 1-2, 2009. **Target date: September 2009.**

3.2 The EIC will provide executive oversight for the development of the Strategic IM Framework (including governance and accountability), Policies, Directives, initiatives and projects. **Target date: December 2009.**

3.3 The Terms of Reference for the EIC will include implementing IM oversight and establishing a formal mechanism, led by National Office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels. **Target date: January 2010.**

3.4 Terms of Reference for the EIC and its supporting working groups, Agendas, Records of Decision, presentations and Forward Agendas will be effectively shared, with all staff via Parks Canada National Intranet (Documents from 1st meeting to be shared in October. (Subsequent meetings to be shared within 2 weeks of the meeting). **Target date: March 2010.**

3.5 The Office of the CIO will take a leadership role in formalizing and chairing monthly meetings with the IM, IS, and IT communities; including some Field Unit representation. The Agenda will focus on IM issues, projects, initiatives, and challenges. Records of Decision will be accessible via the Intranet. **Target date: April 2010.**

> **[4]** The Chief Information Officer should develop an IM training strategy that considers IM training needs based on priority levels, and enhancements required to the online course and other learning/awareness channels. This includes appropriate and specific training and resource material provided to IM staff. Track attendance to IM training, as required.

Management response:

AGREE.
4.1 Attendance, and completion, will be tracked for the on-line IM Awareness and all training provided, or funded, by the OCIO. **Target date: February 2010.**

4.2 Assessment and improvement of the current On-line IM Awareness course. **Target date: March 2010.**

4.3 Develop an IM Training Strategy (including IM Awareness) that addresses needs on a priority basis (e.g. IM Training for IM Specialists) and reflects training requirements by position. **Target date: June 2010.**

6.1.1B Criteria

An IM governance and accountability framework has been implemented, including defined roles and responsibilities.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

At a high level, the PCA IM Policy defines accountability for the CEO, Executive Board, Chief Information Officer (CIO), managers, and all staff, although it does not specify the responsibilities of IM functional specialists (i.e. IM Officers). Those interviewed throughout PCA indicated a lack of awareness of staff roles and responsibilities with respect to information management.

A new IM/IT governance business case is being developed. The national office has a small team of IM professionals and each service centre has two IM Officers. National and service centre IM staff have no formal reporting relationship with each other, or formal mechanism for discussion. A meeting of all IM staff was held in May 2009, although prior to this meeting there had been no formal nation-wide IM meetings for many years. IM and records management roles and resources (i.e., staff) at the field unit level are inconsistent.

The majority of national IM systems are supported by the CIO's office and Service Level Agreements (SLAs) have been developed. These SLAs currently function as Memorandum of Understanding, but do not contain performance indicators. Some program areas indicated a low level of support for those systems that are supported by the CIO office. There are approximately 20 major national systems supported by the CIO office (as identified by the IM/IT Systems Description and Risk Assessment); however, a recent inventory identified over 225 systems/databases in use throughout PCA. These databases and systems have been developed outside the oversight of the CIO at the service centre and/or field unit level. SLAs have not been established for any of these systems. There is no guidance or formal oversight available related to the development of these systems with respect to determining business requirements and assessing appropriate security and privacy controls.

Conclusion

An IM governance and accountability framework has not been implemented. Although accountability for national IT systems exists, it could be strengthened through enhanced SLAs. The majority of systems/databases at PCA have been developed at the service centre/field unit level and outside of the oversight of the CIO office. These current practices diminish accountability and lead to inconsistent and/or inappropriate IM practices.

Recommendations

[3] The Chief Information Officer should develop an IM governance and accountability framework. This includes implementing an IM oversight committee and establishing a formal mechanism, led by national office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels.

Management response:

Same as section 6.1.1A (Page16)

[5] The Chief Information Officer should:

- Ensure national systems can respond to regional needs and these national systems are being fully utilized.
- Review current use of databases at the service centre and field unit level and identify opportunities for these to be eliminated and replaced with existing national systems that offer the same functionality.
- Ensure priority is placed on those activities that have the highest requirements for the business value, confidentiality, integrity and availability of information.
- To the extent 'local' databases may need to be developed, develop guidance and a checklist related to the development of databases that outline IM and other considerations (i.e., determining business requirements and assessing appropriate security and privacy controls).

Management response:

PARTIALLY AGREE.

Some national systems cannot meet all needs. Regional systems will be accepted on an exceptional basis where the required functionality does not exist within the national system.

5.1 CIO will present the National and Regional Systems Inventory to EIC for review. **Target date: May 2010.**

5.2 CIO to develop an information systems solutions prioritization framework to ensure Information Systems and Information Technology priorities are aligned with Agency priorities, regional needs and compliance with Agency's legislated mandate and policies for IM and IT. **Target Date: May 2010.**

5.3 CIO will provide strong governance and accountability by working in collaboration with contracting to include specific terms and conditions applicable to all contracts that state that any contract that includes systems or database development must be approved by the CIO prior to contract award. Owners of national systems should plan regular reviews and surveys of users of systems. The results should be part of the business analysis for modifications. **Target date: June 2010.**

5.4 CIO will develop enterprise architectures for information, business processes, systems, and technology. These frameworks will layout principles and procedures for alignment of business information systems to the Agency's strategic outcomes. **Target date: December 2010.**

6.1.1C Criteria

Training and awareness initiatives related to IM have been implemented.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

IM training and awareness initiatives launched over the last few years have largely been stalled or reduced in scale. Service centre staff indicate they have waited to be provided guidance from national office related to IM training and awareness. An online, non-mandatory IM awareness course has been developed and is available on PCA's Intranet site as of December 2008. Information on who has completed the course is not available. Those interviewed who had completed the course noted that it a good starting point, but that it was generic and/or did not provide enough information on how to actually address the issues of IM. ATIP and/or privacy awareness training has not been conducted for several years. National office IM has indicated hesitation in providing additional training or awareness due to a lack of capacity. Several individuals that were interviewed indicated they had not received any PCA-specific guidance related to IM.

Specific training or resource material has not been provided to IM Officers within the service centers, although many of these individuals have proactively taken IM-related courses through the Canadian School of Public Service (CSPS).

Given the lack of training and awareness, those interviewed indicated that staff do not know what to keep or dispose of, and how to classify or structure data. This results in duplicate or lost information and difficulty in responding to ATIP requests.

Conclusions

Although some training and awareness initiatives have been initiated, additional training and awareness is required related to specific IM issues in the context of individual job functions.

Recommendations

> **[4]** The Chief Information Officer should develop an IM training strategy that considers IM training needs based on priority levels (e.g. Senior Managers involved in strategic decision making, IM Officers), and enhancements required to the online course and other learning/awareness channels; this includes appropriate and specific training and resource material provided to IM staff to help them meet the requirements of their job descriptions. Track attendance to IM training.

Management response:

Same as section 6.1.1A (Page 17)

6.1.1D Criteria

Appropriate IM policies and procedures apply to national, service centre and field unit levels and have been appropriately communicated.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

A PCA IM Policy exists which addresses high-level accountability and requirements for the collection, organization, use, storage, protection, preservation, retention and disposal of information. The policy provides statements related to high-level requirements, many of which may be difficult for PCA staff to comply with given the current IM framework and tools available (i.e., lack of electronic document and records management system and lack of records disposal authority). In general, staff were not aware of the IM policy or its requirements; and to the extent they were familiar with the requirements, they were not sure how to apply them to their daily job activities. Monitoring adherence to the IM policy is not being conducted.

Conclusion

An IM policy has been implemented, although awareness of the Policy is low, and practical guidance on meeting the requirements of the policy has not been provided.

Recommendations

[1] The Chief Information Officer should ensure IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. Within regions, ensure the service centre business plan also considers IM requirements, and that these are incorporated into the yearly planning process conducted between service centres and the field units.

Management response:

Same as section 6.1.1A (Page 15)

[3] The Chief Information Officer should develop an IM governance and accountability framework. This includes implementing an IM oversight committee and establishing a formal mechanism, led by national office IM, to ensure regular communications and meetings are conducted with IM professionals at the national office, service centre, and field unit levels.

Management response:

Same as section 6.1.1A (Page 16)

[4] The Chief Information Officer should develop an IM training strategy that considers IM training needs based on priority levels (e.g. Senior Managers involved

in strategic decision making, IM Officers), and enhancements required to the online course and other learning/awareness channels. This includes appropriate and specific training and resource material provided to IM staff to help them meet the requirements of their job descriptions. Track attendance to IM training.

Management response:

Same as section 6.1.1A (Page 17)

6.1.2 Collection, Creation, Receipt and Capture

6.1.2.A Criteria

The information collected supports PCA objectives and legislative/ program requirements.

YELLOW	Moderate Improvements Needed	Some controls are in place and functioning. However, major issues were noted and need to be addressed. These issues could impact on the achievement or not of program/operational objectives.

Observations

In general, based on our review of a sample of information collected by PCA, the collection of information by program areas is consistent with the requirements of the program areas. While PCA does not centrally manage or classify information and there is no formal process for determining information collection needs, the type of information collected appears to be consistent between the same program areas in different service centres or field units.

For corporate service functions such as Human Resources (HR) and finance, the information collected is driven by national requirements, and where applicable PCA or Federal Government forms. The PCA Intranet has several templates and instructions related to reporting for these functions. For other program areas, although consistent in the information collected, the numerous information collection forms that may be used by field units are not consistent in 'look and feel' and have not been subject to a formal approval process. These forms are generally developed on an ad hoc basis within each field unit. Of specific note, there is no approval process or required consultation with national office or other IM staff related to the development of forms intended to collect personal information (for example, the development of surveys to collect personal information from the public).

The data structure of national IT systems has been based on the business requirements identified during system development, although for smaller systems or databases at the service centre or field unit level this is generally an informal process, and business requirements are not formally captured.

An objective of the PCA Assessment Project (PCAAP) that is currently in progress, and being jointly conducted by PCA and Library and Archives Canada (LAC), includes the identification of business processes and information resources (data and documents), allowing PCA to further determine if the information collected by program areas supports PCA objectives and legislative/ program requirements.

The lack of an approval process for information collection forms increases the risk that forms do not adhere to IM-related legislative and policy requirements, diminishes the perception of a unified message to the public or other stakeholders, and increases the workload as previously developed forms are not leveraged.

.

Conclusion

There is a lack of oversight related to the development and implementation of the processes used to collect information; however, based on our review of a sample of information collected by PCA, the information collected appears to support PCA's objectives and legislative/program requirements.

Recommendations

[5] The Chief Information Officer should:

- Ensure national systems can respond to regional needs and these national systems are being fully utilized.
- Review current use of databases at the service centre and field unit level and identify opportunities for these to be eliminated and replaced with existing national systems that offer the same functionality.
- Ensure priority is placed on those activities that have the highest requirements for the business value, confidentiality, integrity and availability of information.
- To the extent 'local' databases may need to be developed, develop guidance and a checklist related to the development of databases that outline IM and other considerations (i.e., determining business requirements and assessing appropriate security and privacy controls).

Management response:

Same as section 6.1.1B (Page 19)

[6] The Chief Information Officer should create a central forms unit responsible for the creation and management of information collection forms. Only forms developed and approved by this unit should be authorized to be used within PCA. The form unit should ensure forms adhere to legislative and policy requirements, and forms used to collect personal information should be reviewed by ATIP.

Management response:

PARTIALLY AGREE.

Agree that there is a requirement for greater management and coordination of forms; however, structural changes may not be required. A review will be undertaken.

6.1 CIO will, in collaboration with Director's General Eastern and Western and Northern, the Executive Director of the Service Centres, DG ERVE and the CAO to create an Inventory of all Finance, Human Resource, Administration and Social Science forms. The inventory will also include all Treasury Board forms that are applicable to Parks Canada. The CIO will also ensure that a coordinator is assigned to create and update/maintain the inventory. **Target date: June 2010.**

6.2 CIO will develop guides for all staff on the "authoritative source" for the form. **Target date: September 2010.**

6.3 CIO will develop a proposal for the creation of a central forms unit responsible for the creation and management of information collection forms, which will include an action plan. **Target date: September 2010.**

[7] The Chief Information Officer should develop an information asset inventory that captures the key information and its business value and role within PCA, including personal information, in order to update PCA's current PIBs. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their information collection needs and the role and business value of the information collected.

Management response:

AGREE.

7.1 The Manager of ATIP, in collaboration with the Office of the CIO and Business Area representatives, will review current Personal Information Banks (PIBS) in INFOSOURCE and analysis of their accuracy. Business with help of ATIP Office will prepare and publish revisions for existing PIBs. **Target date: June 2010.**

7.2 For all systems in the Systems Inventory, the ATIP Office will ensure that, where applicable, system owners are advised that Privacy Impact Assessments and Threat and Risk Assessments are required for their systems. **Target date: June 2010.**

7.3 The Manager of ATIP, in collaboration with the Office of the CIO, will build processes/services to work with business to conduct privacy strategies for PA1, PA2, PA3 and PA4 and PA5; Privacy Impact Assessments for all new systems used to collect/capture personal information. **Target date: September 2010.**

7.4 PCA has initiated this inventory via the Parks Canada Agency Assessment project where by business units are identifying Information Resources of business value. **Target date: December 2010.**

7.5 The CIO will lead a project to conduct a detailed information asset inventory for PCA that includes all information holdings both electronic and non-electronic. **Target date: December 2011.**

6.1.2.B Criteria

Formal procedures and guidelines have been developed to ensure information is assessed at time of creation related to its role and business value.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

Formal guidance or processes have not been developed related to assessing the business value of information. These considerations are taken at the individual level or by records clerks in a record centre. It appears individuals have an understanding of what information is required to perform their job functions, but to the extent the individual leaves their job or the information is subsequently shared, there is no context available related to the information's business value or role. As information is not assessed at time of creation, it is difficult for individuals after the fact to determine the extent to which information should be retained or disposed. Records centre staff have a significant amount of information in which a determination has yet to be made on the value of the information (as the information was 'dropped off' at the records centre) and the staff do not have context on what information may be important. Without a formal framework to assess the value and role of information, information is not being appropriately classified related to its confidentiality, integrity and availability requirements; given this, appropriate controls to safeguard the information cannot be easily determined. The IM/IT Business Plan indicated a priority was the development of an information asset inventory that depicts the key information of the Agency; this has not yet been developed. An objective of the PCA Assessment Project (PCAAP) is the development of recordkeeping requirements.

Conclusion

PCA has not determined the business value and role of information assets within the Agency, nor have formal procedures and guidelines been developed to ensure information is assessed at time of creation related to its role and business value.

Recommendations

[7] The Chief Information Officer should develop an information asset inventory that captures the key information and its business value and role within PCA, including personal information, in order to update PCA's current PIBs. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their

information collection needs and the role and business value of the information collected.

Management response:

Same as section 6.1.2A (Page 24)

6.1.3 Organization of Information

6.1.3.A Criteria

Recordkeeping repositories have been designated to maintain information resources of business value.

RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

Observations

There is no corporate electronic document and records management (EDRM) system. Current electronic data management practices are inconsistent, as data may be held in network drives (either shared or personal folders), on an individual's desktop, e-mail folder, USB keys, or diskettes. This makes it difficult to appropriately manage information, as staff may not know what information exists and where to find it. This is particularly true for operational information (i.e., correspondence, development of reports). Some program areas have developed national systems intended to manage the information within electronic format, for example the Information Centre on Ecosystems (ICE) serves this purpose for ecological information. Other program areas use a variety of systems across the country (e.g., cultural resources) or have adopted a national system that is not used by all service centres/field units (e.g., asset management system).

Storage of physical records varies across service centres and field units, and some service centre sites and field unit locations do not have a central record centre for hardcopy documents. There is a PCA Central Records at national office that is managed by Canadian Heritage, although program areas within the national office may utilize their own repository (i.e., the National Parks Directorate Documentation Centre). Records centres across PCA are underutilized, in that many program areas do not send any records, although records centres staff indicate they do not currently have the capacity (from a resource and space perspective) to provide services to every program area. In general, the use of records centres is inconsistent and ad hoc.

Other functional areas within a service centre (e.g., HR) have their own designated repositories (i.e., filing cabinets) for their hardcopy records, although they are not always used effectively, as HR information in one instance was found in various locations within a service centre. Reports developed for program areas or field units are not always catalogued or available within the appropriate repository.

The current state of recordkeeping repositories makes it difficult for PCA staff to track or share information. In addition, the lack of appropriate recordkeeping standards increases the risk that information is not appropriately safeguarded from potential damage or inappropriate access.

Conclusion

A consistent framework related to the organization and maintenance of electronic records does not exist. Repositories for hardcopy records exist in some locations, but their use is inconsistent and ad hoc.

Recommendations

[2] The Chief Information Officer should review the long-term purpose and role of the record centres and determine their resource requirements.

Management response:

Same as section 6.1.1A (Page 16)

[8] The Chief Information Officer should develop an information classification standard to ensure the consistent organization of hardcopy and electronic information.

Management response:

AGREE.

8.1 The OCIO, in collaboration with business representatives from each Program Activity Area, will produce an information classification standard (ICS) based on the Agency's functions and activities to be used for hard copy and electronic information resources. **Target date: September 2010.**

[9] The Chief Information Officer should implement an integrated electronic document and record management (EDRM) suite that includes a single point of access to all relevant electronic documents and structured data repositories.

Management response:

PARTIALLY AGREE.

Funding is currently unavailable for implementation of the integrated suite. Planning and implementation for the solution will be based on addressing areas of greatest risk.

9.1 The Office of the CIO is currently piloting a new solution that will improve the efficiency and effectiveness of collaboration. **Target date: On-going.**

9.2 Subject to the availability of funds, the Office of the CIO will conduct user/system requirements analysis and build, or buy, the components of the required suite of tools

(e.g. Records management, Enterprise Search, Collaboration, photo/image management, and digital asset management, e-discovery, metadata for documents, reports, blogs, wikis, geospatial data, electronically stored information repositories). **Target date: March 2012.**

6.1.3.B Criteria

Records and information are organized according to a structured set of business rules and information technology requirements, which prescribe the ways in which records and information must be stored and handled.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

A file classification structure has been developed and is used for the tracking of hardcopy records in records centres through the use of iRIMs (a system for records management). This file classification is only in use with those records held in records centres. PCA does not have a centralized list of information holdings, and there is no file classification structure for electronic records. Guidance on naming conventions for electronic records has been provided by national office IM, although use of these conventions is limited and not consistent. PCA metadata standards are published on the PCA Intranet, although they do not appear to be in use.

There is no formal guidance or processes related to assessing the business value of information, making it difficult to organize records and information according to a structured set of business rules. This makes it difficult for PCA staff to track or share information. In addition, the lack of appropriate standards increases the risk that information is not appropriately safeguarded. Of note, an objective of the PCA Assessment Project (PCAAP), that is currently in progress and being jointly conducted by PCA and Library and Archives Canada (LAC), is the development of recordkeeping requirements.

Conclusion

With the exception of a limited amount of hardcopy records, records are not organized according to a structured set of business rules and information technology requirements, and the ways in which records and information must be stored and handled have not been prescribed.

Recommendations

[8] The Chief Information Officer should develop an information classification standard to ensure the consistent organization of hardcopy and electronic information.

Management response:

Same as section 6.1.3A (Page 27)

[9] The Chief Information Officer should implement an integrated electronic document and record management (EDRM) suite that includes a single point of access to all relevant electronic documents and structured data repositories.

Management response:

Same as section 6.1.3A (Page 27)

6.1.4 Use and Dissemination

6.1.4.A Criteria

Effective use and dissemination of records and 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. Appropriate controls have been implemented related to access to information requests and the sharing of information with third parties.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Observations

Through the use and dissemination of information, program areas appear to be meeting operational requirements, but not necessarily in the most efficient manner. Given the lack of a control framework over electronic information, information can be difficult to find (or lost), may be unnecessarily duplicated, and its accuracy can be challenged. In general, staff could fairly easily find information and reports that they had directly been involved with, other information/reports pertaining to their program areas were difficult to find, although most were located after extended searching.

In general, each program area and field unit has their own standards and methods of collecting and retaining data (i.e., different IM protocols, formats, IT programs/applications used). For example, monitoring programs within National Parks use different (informal) protocols between field units and even within field units for different years. This makes it difficult to identify and report on trends, as well as ensuring accurate information is available for required reporting. Formal IM protocols have not been determined for the majority of these activities. For this type of monitoring information, field staff indicate the Information Centre on Ecosystems (ICE) can act as a repository of information, but does not have the functionality to serve the purposes of day to day collection and tracking of information; this necessitates a variety of 'local' databases and spreadsheets being used within each field unit. Those responsible for ICE have not been tracking compliance with entering data in ICE.

The ATIP function has only been 'brought-back' to PCA as of April 2009; Environment Canada was handling ATIP for PCA from 2005-2008. ATIP requests are now coordinated by ATIP at the national office. Given the current state of IM within PCA, trying to identify all the information that is subject to a request in a timely manner (or at all) can be difficult. As of June 18, 2009 there were 39 access requests considered overdue, with some dating from 2006.

PCA shares information with third parties including other government departments and jurisdictions for purposes such as collaboration on research. In general, Memorandum of Understanding (MOUs) outlining the conditions and terms of these exchanges has not been developed with these third parties. The accountability of PCA and these third parties over the information exchanged is diminished without appropriate MOUs.

Conclusion

IM standards within PCA are not consistent, making the use and disseminating of records and information difficult, this includes the lack of data sharing agreements with third parties. Furthermore, there is a risk PCA is currently not compliant with the requirements of the *Access to Information Act* with regards to timely resolution of access to information requests.

Recommendations

[5] The Chief Information Officer should:

- Ensure national systems can respond to regional needs and these national systems are being fully utilized.
- Review current use of databases at the service centre and field unit level and identify opportunities for these to be eliminated and replaced with existing national systems that offer the same functionality.
- Ensure priority is placed on those activities that have the highest requirements for the business value, confidentiality, integrity and availability of information.
- To the extent 'local' databases may be required, develop guidance and a checklist related to the development of databases that outline IM and other considerations (i.e., determining business requirements and assessing appropriate security and privacy controls).

Management response:

Same as section 6.1.1B (Page 19)

[10] The Chief Information Officer should ensure MOUs are established for all activities involving data sharing with third parties. Develop a process to ensure appropriate approval and oversight is provided for all data sharing activities.

Management response:

AGREE.

10.1 CIO will conduct an Agency-wide survey to determine who is sharing data with whom and to identify where data sharing agreements exist. **Target date: June 2010.**

10.2 Working with Legal services, Departmental security office, ATIP Office, the OCIO will provide guidance on data sharing agreements as well as changes to existing agreements to ensure that the agreements comply with legislation and policies in the jurisdictions. **Target date: December 2010.**

10.3 Directives and procedures for data sharing agreements will be developed. Templates and instructional packages will be created. EIC will approve the directives and procedures, and templates and instructional packages and will provide on-going oversight. **Target date: December 2010.**

> **[11]** The Chief Information Officer should ensure consistent IM protocols are established prior to the collection of information for activities such as monitoring programs.

Management response:

AGREE.

11.1 CIO will develop a protocol and framework with a proposed action plan for the development of the policy instruments that will be presented to EIC. **Target date: March 2010.**

11.2 CIO will develop instruments to help program activity owners to conduct the analysis and apply the instruments starting in the following fiscal years **Target date: September 2012.**

> **[14]** The Chief Information Officer should use the existing ATIP work plan to create a risk-based management framework that considers the structures, policies, systems and procedures to distribute responsibilities, coordinate work, manage risks and ensure compliance with the *Privacy Act* and *Access to Information Act.* Dedicate the necessary resources to ensure the current backlog of access to information requests is addressed.

Management response:

AGREE.

14.1 A review of the backlog of requests is in progress. Senior Managers are being contacted. **Target date: On-going.**

14.2 The Manager of ATIP will develop a framework for Access to Information and Privacy processes will be defined and presented to EIC and Executive Board. It will include defining role of ATIP contacts; procedures for ATIP contacts; responsibilities for Senior Managers and employees; procedures for processing requests; training to ATIP contacts and Senior Managers. **Target date: June 2010.**

6.1.5 Maintenance, Protection and Preservation

6.1.5.A Criteria

Long-term availability, understandability and usability of information assets is maintained.

ORANGE	Significant Improvements Needed	Controls in place are weak. Several major issues were noted that could jeopardize the accomplishment of program/operational objectives. Immediate management actions need to be taken to address the control deficiencies noted.

Requirements

Access to Information Act: Individuals have a right to be given access to any record under the control of a government institution, unless access to the record is exempt based on the provisions contained in the Act. Within thirty days after a request is received the individual must be: i) given written notice as to whether or not access to the record or a part thereof will be given; and, ii) if access is to be given, give the person who made the request access to the record or part thereof. Time extensions may be permissible under specific circumstances.

Observations

The ATIP function has only been 'brought-back' to PCA as of April 2009; Environment Canada was handling ATIP for PCA from 2005-2008. ATIP requests are now coordinated by ATIP at the national office. Given the current state of IM within PCA, trying to identify all the information that is subject to a request in a timely manner (or at all) can be difficult. There is no corporate electronic document and records management (EDRM) system (a pilot for the implementation of an EDRM has been under development for several years). Current electronic data management practices are inconsistent, as data may be held in network drives (either shared or personal folders), on an individual's desktop, e-mail folder, USB keys, and diskettes. This makes it difficult to appropriately manage information, as staff may not know what information exists and where to find it. As of June 18, 2009 there were 39 access requests considered overdue, with some dating from 2006.

Designated hardcopy repositories have varying levels of physical and environmental controls. A library visited during the audit containing many original documents and reports dating back to the 1950s had no environmental controls. Photographs and other historical images are also being stored without proper climate controls. In another location visited, there were sprinklers directly above original (and single copy) hardcopy records related to excavation field notes for artifacts. These field notes are not in an electronic format. Field notes provide detailed information on an excavation and each artifact that were found.

Some records centers and libraries have several boxes containing hardcopy records that have not been inventoried or classified. For those files that have been inventoried and

filed within a records centre, there are inconsistent processes for their 'charging-out' or removal. At one location, no identification or reason for charging out the file was required to be given. Some files have been charged out for years at a time. In some program areas, hardcopy files could not be found that were associated with electronic information within a database (i.e. the database indicated additional information was available in hardcopy format).

Regular backups are performed of IT systems, but there are no documented backup policies or procedures, and practices are inconsistent between locations. In some instances, backup tapes are stored onsite. Some 'local' databases are only backed up to external drives that are stored at the employee's home. Of note, in one of the field units, the server is insecurely located on the floor of the mechanical room.

Some older IT systems are no longer supported by the vendor, and staff indicated the instability of the system has resulted in some information being lost.

Conclusion

Current practices increase the risk that PCA is not compliant with the requirements of the *Access to Information Act*. Current IM practices jeopardize the long-term availability, understandability and usability of information assets.

Recommendations

[7] The Chief Information Officer should develop an information asset inventory that captures the key information and its business value and role within PCA, including personal information in order to update PCA's current PIBs. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their information collection needs and the role and business value of the information collected.

Management response:

Same as section 6.1.2A (Page 24)

[12] The Chief Information Officer should develop IT backup policies and procedures, which should be incorporated as part of a formal business continuity management and disaster recovery plan. As part of this process, review the environmental controls of records centres and server rooms.

Management response:

AGREE.

12.1 CIO will develop IT Back-up policies and procedures for Corporate and National systems and share with IM/IT specialists in Service Centres and Fields Units. **Target date: June 2010.**

12.2 CIO will work with the Departmental Security Officer (DSO) to ensure that the information/data is effectively assessed, and addressed, in Business Impact Assessments (BIAs). Once identified via BIAs, the CIO will ensure that IM/IT requirements are incorporated into the Agency's BCP, and disaster recovery plans will be developed. (Note: this will include a review of the environmental controls of records centers and server rooms.) **Target date: December 2010.**

12.3 CIO will communicate with each Records Office Owner to advise them of their accountabilities related to controlling their environments. The assessments will be done for all Records Offices over the next 3 years. In the first year, focus will be Service Centers and Field Units at risk; Year 2 will be National Office Directorates; and Year 3 will be remaining Field Units. **Target date: December 2010.**

6.1.5B Criteria

Appropriate data privacy and security measures have been implemented based on the sensitivity of the data.

RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

Requirements

Privacy Act s. 4 "*No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution*"

Privacy Act s. 6(1) "*Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information*"

Privacy Act s. 6(2) *"A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible".*

Privacy Act s. 6(3) "*A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information*."

Privacy Act s.7 *"Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or for a purpose authorized under s.8 (2)*"

Privacy Act s. 8(1) "*Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section*."

Privacy Act 10(1) "*The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution*"

Observations

An Access to Information and Privacy (ATIP) Action Plan has been developed by the PCA ATIP Coordinator in order to begin addressing the lack of focus on privacy over the last several years. From 2005-2008 Environment Canada provided ATIP support to PCA. The Action Plan includes initiatives to address PCA's access to information and privacy requirements, although the plan does not contemplate required resources or prioritize the actions based on potential risk

IM privacy and security considerations, or related policy and procedures, have not been formally implemented within PCA. Generally, staff at the field unit level were not aware of privacy and security requirements. For instance, a copy of all occurrences in the occurrence tracking system (OTS) related to a particular National Park was available on the network drive for the National Park, and available to everyone with access to the drive. This included sensitive personal information on individuals involved in incidents that required Park Warden intervention.

Personal information is being collected at the field level without oversight or guidance by national office; for example, the collection of personal information related to students conducting research, and for surveys of visitors to National Parks and Historic Sites. The collection of this personal information is generally not adhering to PCA's legislative and policy requirements (e.g., lack of appropriate notice provided, requirement to register Personal Information Banks (PIBs) in InfoSource). Personal information is also being shared and/or disclosed to third parties without appropriate agreements or oversight. Those conducting social science research (i.e., surveys) within PCA are utilizing an online tool resulting in survey data being stored outside of Canada and thus, not protected by Canadian privacy legislation.

Information is not being classified according to its confidentiality, integrity, and availability requirements per the requirements of the Government Security Policy. Records within PCA are considered either 'Protected' or 'Unclassified', but this classification is not done in a consistent or appropriate fashion. In general, 'Protected' files are not being managed differently from 'Unclassified' files. PCA staff working with 'Secret' documents have not been provided with information or tools required to manage these documents appropriately. There is an awareness that 'Secret' documents should not be saved on network drives; however, staff are working on (but not saving) 'Secret' documents on their desktops (that are connected to the PCA network) and saving these documents to unencrypted USB keys.

Privacy and security assessments (i.e., privacy impact assessments (PIAs) and threat and risk assessments (TRA)) have not been conducted, and several privacy/security weaknesses where identified in national systems, including access restrictions (i.e., PeopleSoft and Occurrence Tracking System) and not adhering to privacy notice requirements (i.e. Campground Reservation System and Research Permit System).

Personal Information Banks in InfoSource for PCA are out of date and/or not accurate.

Conclusion

Current practices significantly increase the risk that PCA is not compliant with the IM-related requirements of the *Privacy Act*. A risk-based privacy and security management framework to ensure adherence to privacy and security requirements has not been implemented.

Recommendations

[6] The Chief Information Officer should create a central forms unit responsible for the creation and management of information collection forms. Only forms developed and approved by this unit should be authorized to be used within PCA. The form unit should ensure forms adhere to legislative and policy requirements, and forms used to collect personal information should be reviewed by ATIP.

Management response:

Same as section 6.1.2A (Page 23)

[7] The Chief Information Officer should develop an information asset inventory that captures the key information and its business value and role within PCA, including personal information in order to update PCA's current PIBs. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their information collection needs and the role and business value of the information collected.

Management response:

Same as section 6.1.2A (Page 24)

[10] The Chief Information Officer should ensure MOUs are established for all activities involving data sharing with third parties. Develop a process to ensure appropriate approval and oversight is provided for all data sharing activities.

Management response:

Same as section 6.1.4A (Page 30)

[13] The Chief Information Officer should, based on Policy requirements, conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) on national systems, with a priority placed on those systems containing the most sensitive personal or other confidential information. Develop a privacy and security

risk assessment policy defining when to conduct a PIA/TRA and a formal process for the completion and approval of PIAs/TRAs.

Management response:

AGREE.

13.1 The Manager of ATIP, in collaboration with the CIO, will conduct an inventory of data systems and hard copy records to identify holdings that contain personal information. Once compiled and prioritized, a project plan will be developed to conduct PIA's and TRA's where required. **Target date: June 2010.**

13.2 The Manager of ATIP will create and publish Personal Information Banks (PIBs) based upon results identified the 2008-2009 Management Accountability Framework report. The ATIP Office have initiated, with business units, the review of existing systems that collect, maintain and report on personal information to create an action plan to conduct privacy and threat and risk assessments, and PIBs. **Target date: June 2010.**

13.3 The Manager of ATIP will develop a directive with procedures linked to existing Treasury Board policies will be developed and approved by Executive Board. ATIP Office, in collaboration with the CIO, will ensure training is integrated into IM Awareness training for manager role. **Target date: June 2010.**

13.4 The Manager of ATIP will develop recommendations to improve the Request for Project Approval (RPA) form by incorporating a step for privacy and threat risk assessments. **Target date: June 2010.**

[14] The Chief Information Officer should use the existing ATIP work plan to create a risked-based management framework that considers the structures, policies, systems and procedures to distribute responsibilities, coordinate work, manage risks and ensure compliance with the *Privacy Act* and *Access to Information Act.* Dedicate the necessary resources to ensure the current backlog of access to information requests is addressed.

Management response:

Same as section 6.1.4A (Page 31)

6.1.6 Disposition

6.1.6.A Criteria

Records that no longer have business value are disposed of or transferred for archiving to Library and Archives Canada

RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

Requirements

Library and Archives of Canada Act s. 12. (1) "*No government or ministerial record, whether or not it is surplus property of a government institution, shall be disposed of, including by being destroyed, without the written consent of the Librarian and Archivist or of a person to whom the Librarian and Archivist has, in writing, delegated the power to give such consents*."

Observations

PCA's Records Disposition Authority was approved in 1972 and has been inactive since 1988. Library and Achieves Canada will not currently take PCA's information holdings. As a result, storage space at the national, service centre and field unit level has become an issue. Retention periods have not been defined, with the exception of those administrative records, which fall under a Multi-Institutional Disposal Authority (MIDA). Staff at the service centre and field unit level indicate they require further guidance on the appropriate use of MIDA, and which administrative records can be disposed under MIDA. In general, all records with the exception of finance and HR records are being retained indefinitely. Given the ad-hoc and inconsistent management of electronic information, individual staff members may be disposing of records without the appropriate authority. One of the two main deliverables of the PCAAP is to develop RDAs for all of the program activities and internal services undertaken by PCA. This project is currently underway.

Conclusion

Current practices increase the risk that PCA is not compliant with the IM-related requirements of the *Library and Archives of Canada Act*. PCA does not currently have a records disposition authority and records are not being disposed of or transferred for archiving to Library and Archives Canada.

Recommendations

> **[15]** The Chief Information Officer should ensure a Records Disposition Authority is approved by Library and Achieves Canada. In the interim provide further guidance on the use of MIDA.

Management response:

AGREE.

15.1 All information holdings of business value will be identified. Retention periods for information holdings will be defined based upon Parks Canada's definition of business value. **Target date: December 2011**.

15.2 Library and Archives Canada will identify Parks Canada information that are of enduring value to Canadians thorough an archival methodology. **Target date: December 2011.**

15.3 Develop the Records Disposition Authority for PCA with Terms and Conditions, which will allow the Agency to dispose (transfer or destroy) Agency specific information. **Target date: December 2011.**

6.1.7 Evaluation/Monitoring

6.1.7.A Criteria

A process has been established to report performance, which includes monitoring compliance and assessing continuous improvement.

RED	Unsatisfactory	Controls are not functioning or are nonexistent. Immediate management actions need to be taken to correct the situation.

Observations

PCA is not currently undertaking any IM monitoring or compliance activities. Although some IM-related policies have been developed at the national level, adherence to these policies is not being monitored or evaluated.

Privacy and security assessments have not been conducted related to any IT systems/database or other program activities involving the collection and/or management of sensitive or personal information. Complaints or breaches related to IM (including privacy) have not been tracked.

Conclusion

PCA has not established a monitoring and reporting regime related to IM.

Recommendations

[4] The Chief Information Officer should develop an IM training strategy that considers IM training needs based on priority levels (e.g. Senior Managers involved in strategic decision making, IM Officers), and enhancements required to the online course and other learning/awareness channels. This includes appropriate and specific training and resource material provided to IM staff to help them meet the requirements of their job descriptions. Track attendance to IM training as required.

Management response:

Same as section 6.1.1A (Page 17)

[16] The Chief Information Officer should ensure that a policy and process for IM-related breaches and incidents is implemented, including their appropriate tracking and follow-up.

Management response:

AGREE.

16.1 CIO will develop policy and process for IM-related breaches and incidents (including mitigation processes/terms and conditions to be included in all 3rd party MOUs related to IM and/or information sharing). **Target date: March 2012.**

16.2 Implement policy and process with appropriate tracking and follow-up. **Target date: March 2012.**

APPENDIX A: AUDIT SUMMARY TABLE

.

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
1. Information Management Planning			
1.A. An IM plan and strategy has been developed and implemented. Resources are sufficient based on the plan and strategy, and IM staffs have the appropriate experience and skills.	**Policy on IM s. 6.1.1** "*departmental programs and services integrate information management requirements into development, implementation, evaluation, and reporting activities*" **Policy on IM s. 6.1.5** "*ensuring electronic systems are the preferred means of creating, using, and managing information*" **Policy on IM s. 6.1.6** "*ensuring departmental participation in setting government-wide direction for information and recordkeeping*"	A high level plan and strategy related to IM have been developed, although the business cases outlining specific IM requirements and how they will be met, as well as required resources, have not been developed. Many IM Officers have retained their librarian roles and do not possess the appropriate experience and training to fulfill the expectations outlined within the job descriptions for IM Officers.	**[1] [2] [3] [4]**
1.B. An IM governance and accountability framework has been implemented, including defined roles and responsibilities.	**Policy on IM s. 6.1.1** "*departmental programs and services integrate information management requirements into development, implementation, evaluation, and reporting activities*" **Policy on IM s. 6.1.7 and IM Directive 6.1** "*Senior executive designated responsible for information management*" **Directive on IM Roles and Responsibilities s. 6.2** "*Managers are responsible for managing information as an integral part of their program and service delivery and as a strategic business resource*" **Directive on IM Roles and Responsibilities s. 6.3** "*All employees are responsible for managing the information they collect, create and use as a valuable asset to support not only the outcomes of the programs and services, but also the department's operational needs and accountability*"	An IM governance and accountability framework has not been implemented. Although accountability for national IT systems exists, it could be strengthened through enhanced SLAs. The majority of systems/databases at PCA have been developed at the service centre/field unit level and outside the oversight of the CIO office. These current practices diminish accountability and lead to inconsistent and/or	**[3] [5]**

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
	Directive on IM Roles and Responsibilities s. 6.4 "*IM functional specialists are responsible for supporting the effective management of departmental information throughout its life cycle*" **Policy on Privacy Protection s. 6.2.2** " *Making employees of the government institution aware of policies, procedures and legal responsibilities under the Act*" (similar to **Government Security Policy s. 10.5**)	inappropriate IM practices.	
1.C. Training and awareness initiatives related to IM have been implemented	**Directive on IM Roles and Responsibilities s. 6.2** "*Managers are responsible for managing information as an integral part of their program and service delivery and as a strategic business resource*" **Directive on IM Roles and Responsibilities s. 6.3** "*All employees are responsible for managing the information they collect, create and use as a valuable asset to support not only the outcomes of the programs and services, but also the department's operational needs and accountability*" **Directive on IM Roles and Responsibilities s. 6.4** "*IM functional specialists are responsible for supporting the effective management of departmental information throughout its life cycle*" **Policy on Privacy Protection s. 6.2.2** " *Making employees of the government institution aware of policies, procedures and legal responsibilities under the Act*" (similar to **GSP s. 10.5**) **DRAFT Directive on Recordkeeping s. 6.1.5** "*Communicating with, and engaging, departmental managers and employees on the risks associated with poor recordkeeping, and their responsibilities for recordkeeping within the department and the GC*."	Training and awareness initiatives have been initiated; however, additional training and awareness is required related to specific IM issues in the context of an individual's job function.	**[4]**
1.D. Appropriate IM policies and procedures apply to national, service centre and field unit levels and have been	**Policy on IM s. 6.1.5** "*ensuring electronic systems are the preferred means of creating, using, and managing information*" **DRAFT Directive on Recordkeeping s. 6.1.4** *"Developing and documenting recordkeeping policies and practices within the department that align with business activities and that address accountability, stewardship, performance measurement, reporting and*	An IM policy has been implemented, although awareness of the Policy is low, and practical guidance on meeting the requirements of the policy has not been provided.	**[1] [3] [4]**

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
appropriately communicated.	*legal requirements*."		
***2.* Collection, Creation, Receipt and Capture**			
2.A. The information collected supports PCA objectives and legislative/program requirements	***Privacy Act s. 4*** "*No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution*"	There is a lack of oversight related to the development and implementation of the processes used to collect information; however, based on our review of a sample of information collected by PCA, the information collected appeared to support PCA's objectives and legislative/program requirements.	**[5] [6] [7]**
2.B. Formal procedures and guidelines developed to ensure information is assessed at time of creation related to its role and business value	**Government Security Policy s. 10.6** Departments must identify information and other assets when their unauthorized disclosure, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*, could reasonably be expected to cause injury to the national interest or private and other non-national interests. **DRAFT Directive on Recordkeeping s. 6.1.1** "*Identify 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."*	PCA has not determined the business value and role of information assets within the Agency, nor have formal procedures and guidelines been developed to ensure information is assessed at time of creation related to its role and business value.	**[7]**
3. Organization of Information			
3.A. Recordkeeping repositories have been designated to maintain information resources of business value	**DRAFT Directive on Recordkeeping s. 6.1.3.1** "*Identifying, establishing, implementing and maintaining recordkeeping repositories where information resources of business value must be stored or preserved whether in a physical or electronic storage space*"	A consistent framework related to the organization and maintenance of electronic records does not exist. Repositories for hardcopy records exist in some locations, but their use is inconsistent and	**[2] [8] [9]**

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
		ad hoc.	
3.B. Records and information are organized according to a structured set of business rules and information technology requirements, which prescribe the ways in which records and information must be stored and handled.	**Policy on IM s. 6.1.5** "*ensuring electronic systems are the preferred means of creating, using, and managing information*" ***Privacy Act* 10(1)** "*The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution*" **Policy on Privacy Protection s. 6.2.15** "*Establishing a privacy protocol within the government institution for the collection, use or disclosure of personal information for non-administrative purposes, including research, statistical, audit and evaluation purposes*." **DRAFT Directive on Recordkeeping s. 6.1.3.2** "*Establishing, using and maintaining taxonomy and/or classification systems to facilitate storage, search and retrieval of information to manage information resources of business value in all formats"*	With the exception of a limited amount of hardcopy records, records are not organized according to a structured set of business rules and information technology requirements, and the ways in which records and information must be stored and handled have not been prescribed.	**[8] [9]**
4. Use and Dissemination			
4.A. Effective use and dissemination of records and 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. Appropriate controls have been implemented related to access to information requests and the sharing of	**Policy on IM s. 6.1.3** "*information is shared within and across departments to the greatest extent possible, while respecting security and privacy requirements*" **Directive on IM Roles and Responsibilities s. 6.3.4** "*treating departmental information in a manner that facilitates access while ensuring privacy and security requirements are met*" ***Privacy Act* s. 6(2) "***A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible".* ***Privacy Act* s.7** *"Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or for a purpose authorized under*	IM standards within PCA are not consistent, making the use and disseminating of records and information difficult, this includes the lack of data sharing agreements with third parties. Furthermore, there is a risk PCA is currently not compliant with the requirements of the *Access to Information Act* with regards to timely resolution of access to information requests.	**[5] [10] [11] [14]**

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
information with third parties.	*s.8*" ***Privacy Act* s. 8(1)** "*Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section*." ***Privacy Act* s. 12-18** With limited exceptions, an individual has the right to accessing their personal information **Policy on Privacy Protection s. 6.2.10** "*Establishing measures, when personal information is involved, to ensure that the government institution meets the requirements of the Privacy Act when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations* (**similar to Government Security Policy 10.4**) **Government Security Policy 10.2** "*Departments must implement this policy [Government Security Policy] when sharing Government of Canada information and other assets ... In these cases, departments must develop arrangements that outline security responsibilities, safeguards to be applied, and terms and conditions for continued participation*." ***Access to Information Act*** Individuals have a right to, be given access to any record under the control of a government institution, unless access to the record is exempt based on the provisions contained in the Act		

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
5. Maintenance, Protection and Preservation			
5.A. Long-term availability, understandability and usability of information assets is maintained	**Policy on IM s. 6.1.4** "*all information is managed to respect user agreements, licensing conditions, or both and for ensuring the relevance, authenticity, quality, and cost-effectiveness of the information for as long as it is required to meet operational needs and accountabilities*" **DRAFT Directive on Recordkeeping s. 6.1.3.3** "*Establishing, implementing and maintaining retention periods for information resources of business value in all formats*"	Current IM practices jeopardize the long-term availability, understandability and usability of information assets.	**[7] [12]**
5.B. Appropriate data privacy and security measures have been implemented based on the sensitivity of the data	***Privacy Act* s. 6(1)** "*Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information*" **Government Security Policy 10.8** "*Departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security screening level*"	A risked-based privacy and security management framework to ensure adherence to privacy and security requirements has not been implemented.	**[6] [7] [10] [13] [14]**
6. Disposition			
6.A. Records are disposed of that no longer have business value or transferred for archiving to Library and Archives Canada	***Privacy Act* s. 6(3)** "*A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information*." ***Library and Archives of Canada Act s.* 12. (1)** "*No government or ministerial record, whether or not it is surplus property of a government institution, shall be disposed of, including by being destroyed, without the written consent of the Librarian and Archivist or of a person to whom the Librarian and Archivist has, in writing, delegated the power to give such consents*."	PCA does not currently have a records disposal authority and records are not being disposed of or transferred for archiving to Library and Archives Canada.	**[15]**

Audit Criteria	Legislative & Policy Requirements	Conclusion	Recommendations
	DRAFT Directive on Recordkeeping s. 6.1.3.4 "*Developing and implementing a documented disposition process for all information resources including those of no business value."* **DRAFT Directive on Recordkeeping s. 6.1.3.5** "*Performing regular disposition activities for records by linking departmental classification systems and retention periods to active Library and Archives Canada Disposition Authorities, where possible, and identifying gaps in disposition coverage where no valid Authorities exist."*		
7. Evaluation/Monitoring			
7.A. Process established to report performance, which includes monitoring compliance and assessing continuous improvement.	**Policy on IM s. 6.1.2** "*ensuring that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of the evolution of policies and programs, and allow for independent evaluation, audit, and review*" **Policy on IM 6.1.8** "*establishing, measuring and reporting on a departmental program or strategy for the improvement of the management of information*" **DRAFT Directive on Recordkeeping s. 6.1.3.2** "*Conduct risk assessments of information resources of business value in terms of Access to Information, security of information, the protection of personal and other confidential information, and legal or regulatory risks that inform planning decisions for the protection of information resources of business value."*	PCA has not established a monitoring and reporting regime related to IM.	**[4] [16]**

APPENDIX B: RECOMMENDATIONS AND MANAGEMENT RESPONSE

Recommendations	Management Response	Target Date
1. IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. Within regions, ensure the service centre business plan also considers IM requirements, and that these are incorporated into the yearly planning process conducted between service centres and the field units.	AGREE. 1.1 The Agency has committed to a new Governance structure for Information Management, Systems and Technology, led by the Enterprise Information Committee (EIC). Its' main responsibilities include reviewing all proposed and, on a prioritized basis, on-going projects/initiatives to ensure that IM requirements are determined and IM-related initiatives, as well as resource requirements, are mapped to these requirements. To ensure Agency-Wide IM requirements are incorporated into IM planning and effective integration of Field unit and service centre and national office IM planning, EIC Membership includes DG East (chair), CFO (Internal Services including Financial Management) and there is a member from each Program Activity, and members from Service Centres and Field Units (East and Western and Northern). 1.2 A strategic plan for PCA IM, IS and IT (IMST Strategic Plan) will be developed and presented to EIC identifying current plans for IM, IS, and IT given current resource levels, as well as options, with associated costs, for providing a sustainable Service for IM. With EIC endorsement, the plan and options will be provided to Finance Committee for consideration/approval. 1.3 National Directorates, Service Centres and Field Units business plans will be reviewed to ensure that IM requirements are incorporated into yearly planning process including business continuity planning conducted between the Service Centres and the Field Units.	October 2009 June 2010 December 2010
2. Review the long-term purpose and role of the record centres and determine their resource requirements.	AGREE 2.1 Parks Canada will negotiate with Canadian Heritage for a cost effective extension (2010-2011) to the existing Memorandum of Understanding for PCH to continue to provide the paper based storage for National Office information holdings; library services in National Office; and, ongoing provision of information systems for the records management system for legacy paper based records and library catalogue.	June 2010

Recommendations	Management Response	Target Date
	2.2 Parks Canada will assess the long term role of the record centres when defining the IM Service Model. The resource requirements for managing records will be defined in the Parks Canada Records Strategy. The assessment of records centres (e.g. National Office Directorates, Regional Service Centres, and Field Units, Library and Archives Canada) will be included in the environmental and organizational scan of existing services and assets.	December 2010
3. Develop an IM governance and accountability framework. This includes implementing an IM oversight committee and establishing a formal mechanism, led by national office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels.	AGREE. 3.1 The Executive Board approved the creation of the Enterprise Information Committee (EIC). The inaugural meeting will occur on September 1-2, 2009. 3.2 The EIC will provide executive oversight for the development of the Strategic IM Framework and IM Policy Framework including governance and accountability, Policies, Directives, initiatives and projects. 3.3 The Terms of Reference for the EIC will include implementing IM oversight and establishing a formal mechanism, led by National Office IM, to ensure regular communications and meetings are being conducted with IM professionals at the national office, service centre, and field unit levels. 3.4 Terms of Reference for the EIC and its supporting working groups, Agendas, Records of Decision, presentations and Forward Agendas will be effectively shared, with all staff via Parks Canada National Intranet (Documents from 1st meeting to be shared in October. Subsequent meetings to be shared within 2 weeks of the meeting). 3.5 The Office of the CIO will take a leadership role in formalizing and chairing monthly meetings with the IM, IS, and IT communities; including some Field Unit representation. The Agenda will focus on IM issues, projects, initiatives, and challenges. Records of Decision will be accessible via the Intranet.	 September 2009 December 2009 January 2010 March 2010 April 2010
4. Develop an IM training strategy that considers IM training needs based on priority levels, and enhancements required	AGREE. 4.1 Attendance, and completion, will be tracked for the on-line IM Awareness and all training provided, or funded, by the OCIO.	 February 2010

Recommendations	Management Response	Target Date
to the online course and other learning/awareness channels. This includes appropriate and specific training and resource material provided to IM staff. Track attendance to IM training, as required.	4.2 Assessment and improvement of the current On-line IM Awareness training and learning products. 4.3 Develop an IM Training Strategy (including IM Awareness) that addresses needs on a priority basis (e.g. IM Training for IM Specialists) and reflects training requirements by position.	March 2010 June 2010
5. - Ensure national systems can respond to regional needs and these national systems are being fully utilized. - Review current use of databases at the service centre and field unit level and identify opportunities for these to be eliminated and replaced with existing national systems that offer the same functionality. - Ensure priority is placed on those activities that have the highest requirements for the business value, confidentiality, integrity and availability of information. - To the extent 'local' databases may need to be developed, develop	PARTIALLY AGREE. Some national systems cannot meet all needs. Regional systems will be accepted on an exceptional basis where the required functionality does not exist within the national system. 5.1 CIO will present the National and Regional Systems Inventory to EIC for review. 5.2 CIO to develop an information systems solutions prioritization framework to ensure Information Systems and Information Technology priorities are aligned with Agency priorities, regional needs and compliance with Agency's legislated mandate and policies for IM and IT. 5.3 CIO will provide strong governance and accountability by working in collaboration with contracting to include specific terms and conditions applicable to all contracts that state that any contract that includes systems or database development must be approved by the CIO prior to contract award. Owners of national systems should plan regular reviews and surveys of users of systems. The results should be part of the business analysis for modifications. 5.4 CIO will develop enterprise architectures for information, business processes, systems, and technology. These frameworks will layout principles and procedures for alignment of business information systems to the Agency's strategic outcomes.	May 2010 May 2010 June 2010 December 2010

Recommendations	Management Response	Target Date
guidance and a checklist related to the development of databases that outline IM and other considerations (i.e., determining business requirements and assessing appropriate security and privacy controls).		
6. Create a central forms unit responsible for the creation and management of information collection forms. Only forms developed and approved by this unit should be authorized to be used within PCA. The form unit should ensure forms adhere to legislative and policy requirements, and forms used to collect personal information should be reviewed by ATIP.	PARTIALLY AGREE. Agree that there is a requirement for greater management and coordination of forms; however, structural changes may not be required. A review will be undertaken. 6.1 CIO will, in collaboration with Directors General East and Western and Northern, the Executive Director of the Service Centres, DG ERVE and the CAO to create an Inventory of all Finance, Human Resource, Administration and Social Science forms. The inventory will also include all Treasury Board forms that are applicable to Parks Canada. The CIO will also ensure that a coordinator is assigned to create and update/maintain the inventory. 6.2 CIO will develop guides for all staff on the "authoritative source" for the form. 6.3 CIO will develop a proposal for the creation of a central forms unit responsible for the creation and management of information collection forms, which will include an action plan.	June 2010 September 2010 September 2010
7. Develop an information asset inventory that captures the key information and its business value and role within PCA, including	AGREE. 7.1 The Manager of ATIP, in collaboration with the Office of the CIO and Business Area representatives, will review current Personal Information Banks (PIBs) in INFOSOURCE and analysis of their accuracy. Business with help of ATIP Office will prepare and publish revisions for existing PIBs.	June 2010

Recommendations	Management Response	Target Date
personal information, in order to update PCA's current PIBs. Based on the inventory, implement standards regarding the management of information based on its value/role (including appropriate controls related to its safeguarding). Develop a process that, on a go forward basis, allows functions/program areas to assess and document their information collection needs and the role and business value of the information collected.	7.2 For all systems in the Systems Inventory, the ATIP Office will ensure that, where applicable, system owners are advised that Privacy Impact Assessments and Threat and Risk Assessments are required for their systems. 7.3 The Manager of ATIP, in collaboration with the Office of the CIO, will build processes/services to work with business to conduct privacy strategies for PA1, PA2, PA3 and PA4 and PA5; Privacy Impact Assessments for all new systems used to collect/capture personal information. 7.4 PCA has initiated this inventory via the Parks Canada Agency Assessment project where by business units are identifying Information Resources of business value. 7.5 The CIO will lead a project to conduct a detailed information asset inventory for PCA that includes all information holdings both electronic and non-electronic	June 2010 September 2010 December 2010 December 2011
8. Develop an information classification standard to ensure the consistent organization of hardcopy and electronic information.	AGREE. 8.1 The OCIO, in collaboration with business representatives from each Program Activity Area, will produce an information classification standard (ICS) based on the Agency's functions and activities to be used for hard copy and electronic information resources.	September 2010
9. Implement an integrated electronic document and record management (EDRM) suite that includes a single point of access to all relevant electronic documents and structured data repositories.	PARTIALLY AGREE. Funding is currently unavailable for implementation of the integrated suite. Planning and implementation for the solution will be based on addressing areas of greatest risk. 9.1 The Office of the CIO is currently piloting a new solution that will improve the efficiency and effectiveness of collaboration. 9.2 Subject to the availability of funds, the Office of the CIO will conduct user/system	On-going

Recommendations	Management Response	Target Date
	requirements analysis and build, or buy, the components of the required suite of tools (e.g. Records management, Enterprise Search, Collaboration, photo/image management, and digital asset management, e-discovery, metadata for documents, reports, blogs, wikis, geospatial data, electronically stored information repositories).	March 2012
10. Ensure MOUs are established for all activities involving data sharing with third parties. Develop a process to ensure appropriate approval and oversight is provided for all data sharing activities.	AGREE 10.1 CIO will conduct an Agency-wide survey to determine who is sharing data with whom and to identify where data sharing agreements exist. 10.2 Working with Legal services, Departmental security office, ATIP Office, the OCIO will provide guidance on data sharing agreements as well as changes to existing agreements to ensure that the agreements comply with legislation and policies in the jurisdictions. 10.3 Directives and procedures for data sharing agreements will be developed. Templates and instructional packages will be created. EIC will approve the directives and procedures, and templates and instructional packages and will provide on-going oversight.	June 2010 December 2010 December 2010
11. Ensure consistent IM protocols are established prior to the collection of information for activities such as monitoring programs.	AGREE. 11.1 CIO will develop a protocol and framework with a proposed action plan for the development of the policy instruments that will be presented to EIC. 11.2 CIO will develop instruments to help program activity owners to conduct the analysis and apply the instruments starting in the following fiscal years.	March 2010 September 2012
12. Develop IT backup policies and procedures, which should be incorporated as part of a formal business continuity management and disaster recovery plan. As part of this process, review the environmental controls of records centers and server rooms.	AGREE. 12.1 CIO will develop IT Back-up policies and procedures for Corporate and National systems and share with IM/IT specialists in Service Centres and Fields Units. 12.2 CIO will work with the Departmental Security Officer (DSO) to ensure that the information/data is effectively assessed, and addressed, in Business Impact Assessments (BIAs). Once identified via BIAs, the CIO will ensure that IM/IT requirements are incorporated into the Agency's BCP, and disaster recovery plans will be developed. (Note: this will include a review of the environmental controls of records centers and server rooms.)	June 2010 December 2010

Recommendations	Management Response	Target Date
	12.3 CIO will communicate with each Records Office Owner to advise them of their accountabilities related to controlling their environments. The assessments will be done for all Records Offices over the next 3 years. In the first year, focus will be Service Centers and Field Units at risk; Year 2 will be National Office Directorates; and Year 3 will be remaining Field Units.	December 2010
13. Based on Policy requirements, conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) on national systems, with a priority placed on those systems containing the most sensitive personal or other confidential information. Develop a privacy and security risk assessment policy defining when to conduct a PIA/TRA and a formal process for the completion and approval of PIAs/TRAs.	AGREE. 13.1 The Manager of ATIP, in collaboration with the CIO, will conduct an inventory of data systems and hard copy records will be conducted to identify holdings that contain personal information. Once compiled and prioritized, a project plan will be developed to conduct PIA's and TRA's where required. 13.2 The Manager of ATIP will create and publish Personal Information Banks (PIBs) based upon results identified the 2008-2009 Management Accountability Framework report. The ATIP Office have initiated, with business units, the review of existing systems that collect, maintain and report on personal information to create an action plan to conduct privacy and threat and risk assessments, and PIBs. 13.3 The Manager of ATIP will develop a directive with procedures linked to existing Treasury Board policies will be developed and approved by Executive Board. ATIP Office, in collaboration with the CIO, will ensure training is integrated into IM Awareness training for manager role. 13.4 The Manager of ATIP will develop recommendations to improve the Request for Project Approval (RPA) form by incorporating a step for privacy and threat risk assessments.	 June 2010 June 2010 June 2010
14. Use the existing ATIP work plan to create a risk based management framework that considers the structures, policies, systems and procedures to distribute responsibilities, coordinate work,	AGREE 14.1 A review of the backlog of requests is in progress. Senior Managers are being contacted. 14.2 The Manager of ATIP will develop a framework for Access to Information and Privacy processes will be defined and presented to EIC and Executive Board. It will include defining role of ATIP contacts; procedures for ATIP contacts; responsibilities for Senior Managers and employees; procedures for processing requests; training to ATIP contacts and Senior	 On going June 2010

Recommendations	Management Response	Target Date
manage risks and ensure compliance with the *Privacy Act* and *Access to Information Act.* Dedicate the necessary resources to ensure the current backlog of access to information requests is addressed.	Managers.	
15. Ensure a Records Disposition Authority is approved by Library and Archives Canada. In the interim provide further guidance on the use of MIDA.	AGREE. 15.1 All information holdings of business value will be identified. Retention periods for information holdings will be defined based upon Parks Canada's definition of business value. 15.2 Library and Archives Canada will identify Parks Canada information that are of enduring value to Canadians thorough an archival methodology. 15.3 Develop the Records Disposition Authority for PCA with Terms and Conditions, which will allow the Agency to dispose (transfer or destroy) Agency specific information.	December 2011 December 2011 December 2011
16. Ensure a policy and process for IM-related breaches and incidents are implemented, including their appropriate tracking and follow-up.	AGREE. 16.1 CIO will develop policy and process for IM-related breaches and incidents (including mitigation processes/terms and conditions to be included in all 3rd party MOUs related to IM and/or information sharing). 16.2 Implement policy and process with appropriate tracking and follow-up.	March 2012 March 2012

APPENDIX C: TIMEFRAME FOR COMPLETION OF ACTIONS PLAN

The audit identifies a total of 16 recommendations to improve the overall IM Management. The CIO proposed an action plan to address all of them. Some of the corrective measures require more than 1 step to achieve the target goal. A total of 47 actions are required to fulfill the proposed action plan. Take note that no action item is planned from April 2011 to March 2012 but a follow up will be done as usual. The following table give a sense of the implementation schedule by action item as stated into the Appendix B.

Summary of actions plan by period			
After 6 months	After 12 months	After 24 months	After 30 months
September 2010	March 2011	March 2012	September 2012
1.1 and 1.2 2.1 3.1 to 3.5 4.1 to 4.3 5.1 to 5.3 6.1 to 6.3 7.1 to 7.3 8.1 9.1 10.1 11.1 12.1 13.1 to 13.4 14.1 and 14.2	1.3 2.2 5.4 7.4 10.2 and 10.3 12.2 and 12.3	 7.5 9.2 15.1 to 15.3 16.1 and 16.2	 11.2
Total 31 66 % implemented	Total 8 83 % implemented	Total 7 98 % implemented	Total 1 100 % implemented