



Industry
Canada

Industrie
Canada

Protected A

Audit Report

Audit of Information Management

Audit and Evaluation Branch

November 2013

Recommended for Approval to the Deputy Minister by the
Departmental Audit Committee on January 30, 2014.

Approved by the Deputy Minister on February 6, 2014.

Table of Contents

LIST OF INITIALISMS AND ACRONYMS USED IN REPORT	1
1.0 EXECUTIVE SUMMARY	3
1.1 BACKGROUND	3
1.2 AUDIT OBJECTIVE AND CONCLUSION	4
1.3 MAIN FINDINGS AND RECOMMENDATIONS	4
1.4 AUDIT OPINION.....	6
1.5 CONFORMANCE WITH PROFESSIONAL STANDARDS.....	7
2.0 ABOUT THE AUDIT	8
2.1 BACKGROUND	8
2.2 OBJECTIVE AND SCOPE	11
2.3 AUDIT APPROACH.....	12
3.0 FINDINGS AND RECOMMENDATIONS	13
3.1 INTRODUCTION	13
3.2 GOVERNANCE STRUCTURES, ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES	13
3.3 IM STRATEGY.....	14
3.4 IM POLICY FRAMEWORK	16
3.5 DEPARTMENTAL BUSINESS PROCESSES, SYSTEMS AND TOOLS.....	17
3.6 IM TRAINING, COMMUNICATION AND AWARENESS	21
3.7 MANAGEMENT RESPONSE AND ACTION PLAN	23
4.0 OVERALL CONCLUSION	24
APPENDIX A: AUDIT CRITERIA	25



List of Initialisms and Acronyms Used in Report

ADM	Assistant Deputy Minister
AEB	Audit and Evaluation Branch
ATIP	Access to Information and Privacy
BCS	Business-based Classification Structure
CAE	Chief Audit Executive
CAS	Comptrollership and Administration Sector
CASAC	Comptrollership and Administration Sector Advisory Committee
CB	Competition Bureau
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
CRP	Corporate Risk Profile
DAC	Departmental Audit Committee
DG	Director General
DM	Deputy Minister
EDRMS	Electronic Documents and Records Management Solution
EPMA	Employee Performance Management Agreement
EX	Executive
GC	Government of Canada
IC	Industry Canada
IIMC	Information and Investment Management Committee
IM	Information Management
IMB	Information Management Branch
IMGAF	Information Management Governance and Accountability Framework
IMPPO	Information Management Policy, Planning and Operations
IRBV	Information Resources of Business Value
IS	Industry Sector
LAC	Library and Archives Canada
MAF	Management Accountability Framework



RDIMS	Records, Document and Information Management System
SITT	Spectrum, Information Technologies and Telecommunications
TB	Treasury Board
TBS	Treasury Board of Canada Secretariat
TWIC	This Week at Industry Canada



1.0 Executive Summary

1.1 Background

Information is a valuable asset that the Government of Canada must manage as a public trust on behalf of Canadians. Effective information management (IM) makes government program and service delivery more efficient, supports transparency, collaboration across organizations, and informed decision-making in government operations, and preserves historically valuable information.

Every government employee is accountable for managing all of the information that he or she creates or collects in the performance of his or her work. This implies organizing information within corporate record systems to protect the integrity of information and ensuring that it is available when required in support of Industry Canada (IC) business, accountability and decision-making. Program heads are responsible for holding their employees accountable for their records management practices and for developing and implementing programs to educate staff on records management goals and requirements.

Two organizations are mandated to set the direction and guide Government of Canada IM practices:

1. **Treasury Board of Canada Secretariat (TBS):** Through its Chief Information Officer Branch, Treasury Board of Canada Secretariat is responsible for policy development, monitoring, management oversight, and leading community development and capacity-building initiatives in IM.
2. **Library and Archives Canada:** Has a mandate to facilitate the management of government information (including published material). It accomplishes this by focusing on the life cycle management of information, including the authorized disposition of government records.

Within IC, the Information Management Branch (IMB) directs and supports a program of IM activities to ensure the effective and efficient management of information. The IMB provides strategic direction and services related to recordkeeping, public access to departmental information, departmental access to commercially published information, as well as IM policy, accountability, governance, planning and reporting.

The 2013-2014 Corporate Plan states that there is a risk that the delivery of IC programs and services will be negatively impacted by inadequate capacity to manage information. The Department will implement and report on activities included in the 2013-2014 Corporate Plan, Sector IM Action Plans, and the Information Management Branch business plan as required to mitigate this risk. IMB has put into place two key building blocks to address the risk and issues noted above, as well as to support the development of products and services such that information will be managed efficiently and effectively as an important business resource at IC:

- The IM Agenda
- The Information Management Governance and Accountability Framework (IMGAF)

The IM Agenda is guided by a number of policies and acts including the TB *Policy on Information Management*. This policy provides guidance on the management of information through its life cycle, and outlines accountabilities and responsibilities in government organizations. The life cycle of information management encompasses the following: planning; the collection, creation, receipt, and



capture of information; its organization, use and dissemination; its maintenance, protection and preservation; its disposition; and evaluation.

The IMB has identified GCDOCS as a cornerstone in achieving the Department's IM Agenda. GCDOCS is the Government of Canada's new enterprise-wide content management solution, designed to ensure standardized electronic document and record management across the public service. A government-wide implementation is being managed as a program by the CIO Branch of TBS.

Changes to the Department's organizational structure and reporting relationships affecting the IMB were announced on May 30, 2013. A new stand-alone sector known as the Chief Information Office was created by merging the Chief Informatics Office and the IMB, which previously was part of the Small Business, Tourism and Marketplace Services sector.

1.2 Audit Objective and Conclusion

In accordance with the approved Industry Canada 2013-16 Multi-Year Risk-Based Internal Audit Plan, the Audit and Evaluation Branch undertook the audit of IM.

The objective of the audit was to provide reasonable assurance that Industry Canada's IM Agenda is operating effectively to enable compliance with relevant legislation and policies, and support efficient business operations by assessing:

1. The adequacy and effectiveness of IM governance and accountabilities.
2. The adequacy and effectiveness of IM processes and tools.
3. The adequacy and effectiveness of IM resource capacity, training and culture.

The scope of the audit included an assessment of key IM activities, processes and controls for unstructured electronic information, such as MSWord documents, spreadsheets, e-mails etc., in the specific areas identified in the audit objective for a sample of sectors within Industry Canada. The audit covered IM activities and processes up to May 31, 2013, unless otherwise noted. For sampling purposes, testing of controls covered the period from April 1, 2012 to May 31, 2013.

The results of the audit revealed that, with some exceptions, Industry Canada's IM governance and accountabilities are operating effectively to support the IM Agenda. However, improvements are required in the areas of IM processes, tools and training to fully support the achievement of the IM Agenda and enable compliance with relevant legislation and policies.

1.3 Main Findings and Recommendations

Governance Structures, Roles, Responsibilities and Accountabilities

Governance structures, roles, responsibilities and accountabilities for IM are defined and assigned to senior management through committee terms of reference to support IM, project management and departmental investments.

IM Strategy

A formal IM strategy, the IM Agenda, has been approved and made available. The IM Agenda includes documentation on the improvement of how information is managed in support of organizational business priorities and operations. The IM strategic planning process includes formal input from each sector, and provides tailored IM action plans on an annual basis.



The IM Agenda is not revised on a regular basis nor is a review cycle for the strategy documented. IM performance metrics are not in place to measure the degree to which IM activities are helping the Department achieve its strategic objectives.

Recommendation 1:

- a) The IMB should develop a process whereby the IM Agenda is periodically reviewed and updated to correspond to current IM needs and priorities.
- b) The IMB should identify the IM activities or components from the IM Agenda and IM plans to be measured to track the progress of the IM program. These measures should be periodically reviewed and reported on.

IM Policy Framework

The IC IM policy instruments address IM life-cycle requirements and are developed and communicated through governance committees, the IM Corporate Plan, the intranet and the IC Wiki.

The IC *Directive on Recordkeeping Responsibilities* has not been formally approved and is in draft format.

Recommendation 2:

The CIO should strengthen the IM policy framework by ensuring that IC IM policy instruments are finalized, formally approved, and reviewed on a regular basis.

Departmental Business Processes, Systems and Tools.

IM tools (i.e. checklists, directory structures, processes and procedures) do not fully support all phases of the IM life cycle and supporting processes, including retention and disposition, and storage of sensitive information.

Retention and disposition processes were inconsistently executed for a sample of sectors within the Department.

Security classification was not consistently applied to sensitive information and sensitive information was stored on shared drives for a sample of sectors within the Department.

Recommendation 3:

- a) Under the guidance of the IMB, sectors should review and update business processes related to identification, file closing, retention and disposition of information to ensure they are in accordance with established requirements. They should create tailored enablers (i.e. templates, checklists and criteria) that support the identification of information resources of business value (IRBV).
- b) Under the guidance of the IMB, sectors should review, finalize and periodically update retention and disposition schedules.
- c) Under the guidance of the CIO, and IC Security Services CMS, departmental sectors should develop processes to monitor that the identification and marking of sensitive information is compliant with policy and that appropriate safeguarding measures are considered at all times during the lifecycle of the information.



Process gaps were noted with identification, retention and disposition of IRBV. Existing process gaps will not be fully addressed by the introduction of new IM tools (i.e. GCDOCS).

Recommendation 4:

The CIO should ensure that key business processes integrate with functionality of new IM tools (i.e. GCDOCS) to support business unit needs and enable compliance with IM legislation and policies. IM tools functionality should enable and/or further automate:

- Retention and disposition
- Security classification
- IRBV identification
- Document version control
- Defining authoritative versions of documents
- Declaring documents as “closed”
- Elimination of duplicate information

IM Training, Communication and Awareness

The IMB Outreach Plan, which also describes training efforts, is aligned with the IM strategy and addresses awareness and training requirements issued by the Treasury Board of Canada Secretariat. IM training, communication and awareness plan and respective materials are in place to promote effective IM practices, including document classification.

Interviews with IMB and sector executives indicated that there is a lack of awareness among the Department’s employees of their IM roles and responsibilities. Of the survey respondents, 73% stated that additional IM training would be beneficial to better fulfill their job responsibilities.

Recommendation 5:

Employees should receive mandatory IM training on the following topics:

- IM roles and responsibilities
- The IM life cycle
- Information retention and disposition processes
- Classification of sensitive information

1.4 Audit Opinion

In my opinion, Information Management at Industry Canada has weaknesses, with moderate risk exposures that require management’s attention. Improvements are needed in the areas of policy and strategic direction, business process design and integration, and training.



1.5 Conformance with Professional Standards

This audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada, as supported by the results of the Audit and Evaluation Branch's quality assurance and improvement program.

Susan Hart

Chief Audit Executive, Industry Canada

2.0 About the Audit

2.1 Background

In accordance with the approved Industry Canada 2013-14 to 2015-16 Multi-Year Risk-Based Audit Plan, the Audit and Evaluation Branch (AEB) undertook the Audit of Information Management.

Information is a valuable asset that the Government of Canada (GC) must manage as a public trust on behalf of Canadians. Effective IM makes government program and service delivery more efficient, supports transparency, collaboration across organizations, and informed decision-making in government operations; it also preserves historically valuable information.

Each employee with the government is accountable for managing all of the information that he or she creates or collects in the performance of his or her work. This implies organizing information within corporate record systems to protect the integrity of information and ensuring that it is available when required in support of IC business, accountability and decision-making. Program heads are responsible for holding their employees accountable for their records management practices and for developing and implementing programs to educate staff on records management goals and requirements.

Two organizations are mandated to set direction and guide Government of Canada IM practices:

1. **Treasury Board of Canada Secretariat (TBS):** Through its Chief Information Officer Branch (CIOB), the TBS is responsible for policy development, monitoring, management oversight, and leading community development and capacity building initiatives in IM.
2. **Library and Archives Canada (LAC):** LAC has a mandate to ensure that collection and preservation of Canada's documentary heritage, including government records and to facilitate the management of government information, including the authorization of the disposition of government records.

As per the Treasury Board *Policy on Information Management* and the *Directive on Information Management Roles and Responsibilities*, within each department, the following personnel have specific roles regarding IM:

- Deputy head
- Senior executive for department designated responsible for IM by the deputy head (i.e. Information Management Branch)
- Managers of all levels
- Employees of the Government of Canada

Within IC, IMB directs and supports a program of IM activities to ensure the effective and efficient management of information. The IMB provides strategic direction and services related to recordkeeping, public access to departmental information, departmental access to commercially published information, and IM policy, accountability, governance, planning, and reporting.

Changes to the Department's organizational structure and reporting relationships affecting the IMB were announced on May 30, 2013. A new standalone sector known as the Chief Information Office sector was created by merging the Chief Informatics Office and the IMB from the Small Business, Tourism and Marketplace Services sector.



The IMB has a multi-faceted responsibility for IM, addressing the needs of several distinct clients, including:

- Assisting senior management in setting IM strategic direction through high-level IM governance, accountability, policy and planning framework that relates directly to IC program outcomes.
- Supporting program heads in the implementation of IM within the context of their business activities through the provision of integrating mechanism, IM standards, guidelines and tools.
- Assisting staff in the application of these mechanisms by providing advice and guidance including awareness and training.

The IMB delivers its activities through three service delivery organizations:

- **Library Knowledge Centre:** offers staff the latest electronic resources, specialized commercial databases, library networks and media monitoring services.
- **Information and Privacy Rights Administration:** responsible for the implementation and management of the Access to Information and Privacy (ATIP) programs and services.
- **Information Management Policy, Planning and Operations (IMPPPO):** responsible for departmental IM planning, reporting, outreach and governance, records management services, information architecture, as well as developing IM tools and applications to support business needs.

The audit work focused on:

- the IMPPPO directorate within the IMB, which is responsible for departmental IM planning, reporting, outreach and governance as well as developing IM tools and applications to support business needs, and
- the department's understanding and application of IM in areas of awareness, information resources of business value (IRBV) identification, retention and disposition, and classification.

The 2013-2014 Corporate Plan states that there is a risk that the delivery of IC programs and services will be negatively impacted by inadequate capacity to manage information. The Department will implement and report on activities included in the 2013-2014 Corporate Plan, Sector IM Action Plans, and the Information Management Branch business plan as required to mitigate this risk.

The IMB has put into place two key building blocks to address the risk and issues noted above, as well as to support the development of products and services such that information will be managed efficiently and effectively as an important business resource at IC:

- The IM Agenda
- The Information Management Governance and Accountability Framework



The IM Agenda, which was approved in 2008, sets out the strategic long-term direction for IM in the Department. The objective is consistent with the TB *Policy on Information Management*, as well as desired outcomes in three areas:

- Governance structures, policies and guidelines are in place to support information management
- Employees are aware of their IM responsibilities and know how to execute them
- Employees are given the tools to execute their IM responsibilities

The IMGAF, which was first approved in 2010, supports the Department's IM Agenda by providing for effective decision-making, coordination and oversight of IM initiatives. As defined in the framework, managers, supervisors and employees across the department all have specific responsibilities regarding the management of information. The IMGAF is subject to review every three years to ensure continued relevance. The first such review started in April 2013 and an updated IMGAF was released in Q3 of 2013-14.

The implementation of the IM Agenda takes a multi-year (2008-15) approach set out in four phases. Each phase contains specific initiatives and activities that are laying the IM foundation for the Department.

The IM Agenda is guided by a number of policies and acts including the TB *Policy on Information Management*. This policy provides guidance on the management of information through its life cycle, and outlines accountabilities and responsibilities in government organizations. The life cycle of information management encompasses the following: planning; the collection, creation, receipt, and capture of information; its organization, use and dissemination; its maintenance, protection and preservation; its disposition; and evaluation. Associated with this policy is the TB *Directive on Recordkeeping* with which all government departments must be in compliance by March 31, 2015. The objective of this directive is to ensure effective recordkeeping practices that enable departments to create, acquire, capture, manage and protect the integrity of information resources of business value. Information resources of business value (IRBV) are records that are created or acquired to support decision making and provide evidence of business activities. They enable decision making and the delivery of programs, services and ongoing operations, and support departmental reporting, performance and accountability requirements.

In support of the IM Agenda, the IMB has undertaken the Business-based Classification Structure (BCS) initiative with some of the sectors' business units. The BCS is a record-naming and filing system for the management of information on the Department's shared drives. Stated benefits associated with the BCS project include cleaned up shared drives, better IM awareness and improved search and retrieval of electronic information.

GCDOCS is the Government of Canada's chosen electronic documents and records management solution. GCDOCS is intended to replace the Department's current document repository shared drives and the Records, Document and Information Management System (RDIMS). This is a government-wide implementation and is being managed as a program by TBS CIOB. IMB has identified GCDOCS as a cornerstone in achieving the Department's IM Agenda.



The 2012-13 IC Corporate Information Management Plan was endorsed by the Information and Investment Management Committee (IIMC) and published in April 2012. The 2013-14 planning exercise included input from all sectors and individualized action plans were developed for each sector establishing their IM priorities and activities for the year.

The IMB has drafted a new departmental *Directive on Recordkeeping Responsibilities*. The objectives of this directive will be to:

- Identify IM activities which must be accomplished to ensure the effective management of records of business value.
- Clarify the recordkeeping responsibilities that individuals must undertake to meet their IM accountabilities.

2.2 Objective and Scope

The objective of the audit was to provide reasonable assurance that Industry Canada's IM Agenda is operating effectively to enable compliance with relevant legislation and policies, and support efficient business operations by assessing:

1. The adequacy and effectiveness of IM governance and accountabilities.
2. The adequacy and effectiveness of IM processes and tools.
3. The adequacy and effectiveness of IM resource capacity, training and culture.

The scope of the audit included an assessment of key IM activities, processes and controls for unstructured electronic information in the specific areas identified in the audit objective for a sample of sectors within IC. The sample of sectors determined during the execution phase included:

- Competition Bureau (CB)
- Comptrollership and Administration Sector (CAS)¹
- Industry Sector (IS)
- Spectrum, Information Technologies and Telecommunications (SITT)

The audit covered IM activities and processes up to May 31, 2013, unless otherwise noted. For sampling purposes, testing of controls covered the period from April 1, 2012 to May 31, 2013. The audit excluded:

- User access rights to systems and data, including controls for granting, modifying, revoking and monitoring user access.
- Structured data – such as data captured in the Integrated Financial and Materiel System (IFMS) or the Human Resource Management System (HRMS).
- Library and Knowledge Centre, and IM procurement activities.
- Access to Information and Privacy (ATIP) processes.

¹ CAS has since been merged with the Human Resources Branch into the Corporate Management Sector (CMS)



2.3 Audit Approach

This audit was conducted in accordance with the *Internal Auditing Standards for the Government of Canada* and the *TB Policy on Internal Audit*. The audit procedures followed and the data collected are sufficient and appropriate to attest to the accuracy of the conclusion and the opinion expressed in this report. This opinion is based on a review of the situations identified in time and place, based on pre-established audit criteria agreed upon with management. This opinion applies only to the area under audit and described in the report.

The audit was performed in three phases: planning, conduct and reporting. A risk assessment was executed during the planning phase of this audit to confirm the audit objective and identify areas requiring more in-depth review during the conduct phase. In addition to the risk assessment, the audit team considered the Treasury Board Secretariat's Management Accountability Framework tool for assessing Core Management Controls (CMC).

Based on the identified risks and the CMC assessment, AEB developed audit criteria that linked back to the overall audit objective (refer to Appendix A).

The methodology used to address the audit's objectives included:

- Documentation review
- Survey
 - 1,639 people surveyed
 - 654 people responded (40.0%)
- Interviews with personnel with IM accountabilities and responsibilities
 - 22 people interviewed
- Controls testing of electronic documents
 - Retention and disposition
 - Security classification and storage

The sample sizes selected for controls testing were based on the overall population size during the sampling period and the level of evidence required to conclude on the overall audit criteria.

A debrief meeting was held with IMB management on November 13, 2013 to validate the accuracy of the findings contained in this report.



3.0 Findings and Recommendations

3.1 Introduction

This section presents detailed findings from the Audit of Information Management. The findings are based on evidence and analysis from the initial risk assessment and the detailed audit work.

In addition to the findings below, AEB has communicated to management either verbally or in a management letter, findings for consideration that were either non-systemic or of low risk.

3.2 Governance structures, roles, responsibilities and accountabilities

Governance structures, roles, responsibilities and accountabilities for IM are defined and assigned to Senior Management through committee terms of reference to support IM, project management and departmental investments.

Well-defined governance structures, roles, responsibilities and accountabilities help to guide how an organization or function is managed, delivers value and protects against risk. Additionally, governance structures contribute to effective decision-making and communication across the organization.

Interviews and documents reviewed indicated that governance structure, roles, responsibilities and accountabilities are defined and assigned to senior management through committee terms of references to support IM, project management and departmental investments. Auditors reviewed the terms of reference for the following governance and advisory committees:

- **Information and Investment Management Committee:** The mandate of IIMC is to provide the deputy minister with strategic advice on information technology, IM and Industry Canada's project portfolio prioritization. Membership is comprised of senior level management (i.e. assistant deputy ministers and director generals) and includes the chief financial officer and the chief information officer.
- **Comptrollership and Administration Sector Advisory Committee (CASAC):** The mandate of CASAC includes reviewing, discussing and providing advice on IM issues, proposals and initiatives that have an impact on business resource planning. Membership is comprised of CAS director generals and representatives at the director general or Executive/Senior Director levels from each sector.

The terms of reference for each governance and advisory committee defined the following key elements:

- Decision authority
- Frequency of meetings
- Mandate
- Membership
- Roles



While the IIMC and CASAC were in place during the audit period (April 1, 2012 to May 31, 2013), a new governance structure was subsequently introduced in the Department in September 2013. Mandates and responsibilities to support IM, project management and investments have been transferred to the new committees, which include the:

- Management Committee
- Investment Board
- Director General Management Advisory Committee

Consistent with the information obtained through interviews, the survey results indicate that management and executives understand the roles and responsibilities for IM. Specifically, out of 49 executive-level survey respondents:

- 42 (86%) agreed that they are aware of and understand IM policies, principles and recordkeeping best practices.
- 40 (82%) agreed that their IM roles and responsibilities had been clearly defined and communicated to them.

3.3 IM Strategy

A formal IM strategy, the IM Agenda, has been approved and made available. The IM Agenda includes documentation on the improvement of how information is managed in support of organizational business priorities and operations. The IM planning process includes formal input from each sector, and provides sector-tailored IM action plans on an annual basis.

Strategic planning can be described as an organization's process for defining its strategy, or direction, and making decisions on allocating its resources to pursue this strategy. Strategic planning is important because it directly influences which goals, objectives and priorities resources will be allocated to work towards. IM strategic planning should be aligned with Department and Government of Canada priorities to promote efficient and effective resource allocation focused on IM activities that contribute to these key priority areas.

The current IM strategy, the IM Agenda, has been approved, made available and includes documentation on the improvement of IM in support of departmental priorities and operations. The IM Agenda considered key IM risks, as identified through the Management Accountability Framework (MAF) self-assessment and the Corporate Risk Profile (CRP).

An annual IC IM Corporate Plan (the Plan) is in place that supports the implementation of the IM Agenda. The Plan describes key IM priorities and provides a Department-wide view of the IM activities planned for the fiscal year. The Plan considered key risks as identified through the CRP for the relevant IM capability requirements. The audit compared the Plan with departmental and GC IM priorities issued by TBS. Alignment was found with the priorities and objectives related to the Government of Canada transformation for how information is stored, managed and disposed.

While it is important that key documents such as the IM Agenda and IC IM Corporate Plan are aligned with Department and Government of Canada priorities, it is also essential that strategic planning takes sector considerations into account, including IM issues, focus areas and needs.

The annual IM planning process includes interaction between the IMB and the sectors. The IMB works with each sector to gather input, and subsequently receives sector-tailored IM action plans. Sector-specific IM action plans are signed in agreement by executives of both the IMB and each sector to promote buy-in and teaming from both parties.

As of 2013-14, IM planning has been integrated into the IC corporate planning process, which helps ensure that IM priorities are being presented and prioritized at the corporate level.

The IM Agenda is not revised periodically and no review cycle for the strategy is documented. IM performance metrics are not in place to measure to what degree IM activities are helping the Department achieve its strategic objectives.

Due to the dynamic nature of business, technology and people, it is important to keep business strategies, such as the IM Agenda, up to date. The IM strategy must adapt and evolve with changes in factors such as business structure, technology capability, resource availability and the overall IM landscape.

The IM Agenda has not been reviewed or updated since 2008, and interviews with IMB management indicated that a formal review cycle for the IM Agenda has not been defined.

Having an IM agenda that has not been reviewed or updated since 2008, coupled with the lack of a formal review process, increases the risk that:

- The IM Agenda is not reflective of current IM requirements and priorities; and
- IM activities are not aligned with the Department's strategic objectives for IM.

Well-defined performance metrics and a performance measurement strategy allow organizations to continuously monitor and assess the results of programs, make informed decisions and take appropriate action in a timely manner.

Although the IMB is planning on developing a record keeping performance management strategy, there are currently no IM performance metrics designed and an IM performance measurement strategy is not in place.

Due to the lack of performance metrics and performance measurement strategy, the IMB cannot measure to what degree IM activities are helping the Department achieve its strategic objectives, leading to missed opportunities to leverage IM to improve business performance.

Recommendation 1:

- a) The IMB should develop a process whereby the IM Agenda is periodically reviewed and updated to correspond to current IM needs and priorities.
- b) The IMB should identify the IM activities or components from the IM Agenda and IM plans to be measured to track the progress of the IM program. These measures should be periodically reviewed and reported on.

3.4 IM Policy Framework

Industry Canada IM policy instruments address IM life cycle requirements and are developed, and communicated through governance committees, the IM Corporate Plan, the intranet and the Industry Canada Wiki. However, the *IC Directive on Recordkeeping Responsibilities* was not formally approved and is in a draft format.

A departmental IM policy framework that is aligned to the Treasury Board IM requirements is important to providing the foundation for effective IM governance and IM investment decision-making. A foundation for effective IM governance and investment decision-making, supports decisions that are focused on areas of current IM emphasis. The foundation leads to the execution of effective and efficient activities, and investments that are aligned with government-wide IM objectives.

Auditors reviewed the IC IM policy framework which includes the following policy instruments:

- IC Records Management Policy (2001)
- IC Directive on Recordkeeping Responsibilities (draft copy). This directive is intended to replace the above-mentioned 2001 policy.
- IC Information Management Governance and Accountability Framework (2010)
- IC IMGAF (2013)

The IMB plans to submit the draft version of the IC Directive on Recordkeeping Responsibilities for approval in Q3 2013-2014.

IC has taken a number of steps to improve the alignment of IM policy framework with the Treasury Board policy and directive requirements:

- IC IM policy instruments are drafted to address IM life cycle requirements.
- IC IM policy instruments are developed and communicated through governance committees, the IM Corporate Plan, the intranet and the Industry Canada Wiki.
- IC IM policy instruments are reviewed through the 3-year cycle revision of the IMGAF and through the IMB Quality Assessment, which is triggered when TB introduces changes to IM policies.
- The IC IM policy instruments are created to complement and clarify the TB IM policy and guidelines. For example, the draft IC Directive on Recordkeeping Responsibilities clarifies the responsibilities of all departmental employees in supporting the deputy head in effective management of records at Industry Canada as stipulated in the TB Directive on Recordkeeping. They also describe the IM accountabilities and responsibilities throughout the Department (e.g., DM, CIO, ADMs, DGs, employees).
- The responsibility for monitoring IM program activities to determine whether desired outcomes are achieved is defined in IC IM policy instruments.
- IM guidelines and procedures for the use of collaborative software (i.e. wiki and social media) have been developed and communicated.

We noted that the IC *Directive on Recordkeeping Responsibilities* was not formally approved and is in draft format. The Treasury Board *Directive on Recordkeeping* came into effect on June 1, 2009 and the IC *Directive on Recordkeeping Responsibilities* was originally slated for approval in 2012-13. There is a risk that employees are not aware of their recordkeeping responsibilities or how to execute those responsibilities due to the lack of an approved and communicated departmental directive.

Recommendation 2:

The CIO should strengthen the IM policy framework by ensuring that Industry Canada IM policy instruments are finalized, formally approved, and reviewed on a regular basis.

3.5 Departmental Business Processes, Systems and Tools

IM tools do not fully support all phases of the IM life cycle and supporting processes, including retention and disposition, and storage of sensitive information.

For effective information management at Industry Canada, IM tools should be agile, respond to the business needs, and be easily integrated into existing business processes. Providing effective IM tools (i.e. checklists, directory structures, processes and procedures) to users enables them to address their responsibilities for ownership of information, and minimizes the duplication of information. Ultimately, effective IM tools should facilitate decision-making by providing accurate and reliable information to decision-makers as and when required.

Through interviews, auditors found that some technology was being improperly used to store information, including:

- **Employees' local hard drives:** Sector employees use their local drives to store information instead of the BCS (a shared directory structure created by the IMB to guide how unstructured data is stored in shared network drives) which poses a challenge for knowledge sharing, knowledge transfer and version control.

Interviews, documentation reviews and testing identified that there are process gaps with IRBV identification, retention and disposition.

Various risks were identified due to the lack of adherence to processes for identification, retention and disposition of IRBV, which include:

- ATIP responses taking a greater level of effort than should be required.
- Sectors not being able to completely or accurately respond to ATIP requests, because they do not have a complete understanding of what information they have, where it is stored or who is the information owner.
- Limitation of programs to retain and transfer valuable business knowledge to others within the organization, leading to missed opportunities to improve the overall effectiveness of programs and improve business performance.

Auditors assessed the retention and disposition process for a sample of sectors and examined a sample of potentially sensitive documents stored on the shared drives.



Retention and disposition

Retention and disposition processes were inconsistently executed for a sample of sectors within the Department.

A properly formulated retention schedule includes a retention period and a retention trigger for all types of records created by the sector. The retention period is the period of time information resources are kept before they can be legally disposed of. The retention trigger is the action that initiates the start of the retention period.

Having a properly formulated retention schedule helps prevent the accumulation of obsolete and transitory records and promotes the availability and use of electronic records for appropriate periods of time. It will also make more efficient use of electronic storage media. Some of the sectors did not have retention and disposition schedules established.

Thirty-two documents were assessed to determine whether the documents were managed in accordance with the established retention and disposition schedules for some of the sectors. The following table outlines the results of the testing.

Electronic documents tested		Total
◆	Document still within retention period.	1
◆	Document inappropriately retained beyond retention period.	18
◆	Unable to determine if document was properly retained. Trigger and retention period were not defined for the directory containing the document.	13
Total samples tested		32

Classification of sensitive information

Security classification was not consistently applied to sensitive information and sensitive information was stored on shared drives for a sample of sectors within the Department.

Through testing of compliance with the rules for handling of sensitive information, auditors found Protected B and above documents stored on shared drives in violation of Industry Canada guidelines (i.e. IC's *Guide to the Handling, Storage and Destruction of Protected and Classified Information*). Auditors also identified several misclassified Secret documents stored on shared drives under Protected B, Protected A, and unclassified security levels.

From the departmental shared network drives, a sample of 32 files was selected for testing. The sample files were selected from a list of files that had keywords in their file names that potentially signified that the files' contents included sensitive material. For each sample file, the contents of the file were reviewed to determine whether the document had been marked with the correct security classification and whether the document was stored in a location that meets security requirements.



The Industry Canada network, where these files had been stored, has been accredited for the storage of unencrypted information up to the level of Protected A.

The following table outlines the results of the testing.

Electronic documents tested		TOTAL
◆	Document was sensitive and classified in accordance with guidance	11
◆	Document was not sensitive and classified in accordance with guidance	9
◆	Total documents classified in accordance with guidance	20
◆	Document was sensitive and not classified in accordance with guidance	12
Total of samples tested		32

Of the 12 sensitive documents that were not classified in accordance with IC’s guidance, six documents were assessed to contain Protected information and six documents were assessed to contain Classified information.

Electronic documents tested		TOTAL
◆	Document was stored in accordance with guidance	12
◆	Document was not stored in accordance with guidance	20
Total of samples tested		32

Of the 20 documents that were not stored in accordance with guidance, seven documents contained Protected information and 13 documents contained Classified information. Therefore, their storage on the shared drive is a violation of policy and increases the chance of exposure of sensitive information.

Through interviews, senior management indicated that current tools do not support proper storage of sensitive information. However, in collaboration with the CIO, they have implemented mitigation strategies to minimize the risk of exposure of sensitive information. These strategies include but are not limited to: 1) securing documents through encryption or password protection and 2) limiting document access to a designated group of individuals through IT access rights control. The audit did not verify the effectiveness of these mitigation strategies.



Recommendation 3:

- a) Under the guidance of the IMB, sectors should review and update business processes related to identification, file closing, retention and disposition of information to ensure they are in accordance with established requirements. They should create tailored enablers (i.e. templates, checklists and criteria) that support the identification of information of business value.
- b) Under the guidance of the IMB, sectors should review, finalize and periodically update retention and disposition schedules.
- c) Under the guidance of the CIO, and IC Security Services CMS, departmental sectors should develop processes to monitor that the identification and marking of sensitive information is compliant with policy and that appropriate safeguarding measures are considered at all times during the lifecycle of the information.

Process gaps were noted with identification, retention and disposition of information resources of business value. Existing process gaps will not be fully addressed by new IM tools (i.e. GCDOCS)

Auditors identified the following IM process gaps through interviews and observation:

- **Identifying IRBV:** Some employees have a limited understanding of what defines an IRBV. Considering the Department will be implementing GCDOCS, there is an opportunity to seek input from sectors to help determine the particular requirements for identifying IRBV within each sector.
- **Closing records:** In many cases, the trigger for a retention and disposition period to begin is when a file is properly closed. However, while a process for closing files exists, it is not consistently executed. Failure to close files will prevent the file from being disposed in accordance with the retention and disposition plans.
- **Disposing of records:** Although some sectors have implemented file retention and disposition schedules, information is not regularly disposed of in accordance with the set schedules. A process is not in place to review and update these retention schedules on a periodic basis.

The inability to efficiently and effectively store data, and translate this data to relevant and accessible information using IM tools can result in:

- Inefficiencies in the work conducted by the Department, which includes the cost of storing information beyond its retention period
- Hindered IM performance measurement processes
- Impaired decision making and missed opportunities
- Inadequate knowledge management, which is central to IC's mission to foster a knowledge-based Canadian economy

Given that the Government of Canada is transitioning to a standard solution for document management, several IM processes will require refining as IC's overall IM framework continues to mature. Accordingly, the Department is in position to consider the opportunities for improvement and establish a greater degree of consistency in IM practices and improved collaboration amongst the sectors.



The transition to a standard solution is an externally driven event that represents both opportunities and threats to the Department. Specifically, IC is made up of numerous agencies with diverse mandates, which may be more challenging to transition to a common platform. Therefore, it is important that IC be proactive in assessing how business processes should be designed to integrate with new IM tools to support and enable compliance with IM policies.

Recommendation 4:

The CIO should ensure that key business processes integrate with functionality of new IM tools (i.e. GCDOCS) to support business unit needs and enable compliance with IM legislation and policies. IM tools functionality should enable and/or further automate:

- Retention and disposition
- Security classification
- IRBV identification
- Document version control
- Defining authoritative versions of documents
- Declaring documents as “closed”
- Elimination of duplicate information

3.6 IM Training, Communication and Awareness

The IMB Outreach Plan, which also describes training efforts, is aligned with the Department’s IM strategy and addresses TB awareness and training requirements. IM training, communication and awareness plan and materials are in place to promote effective IM practices, including document classification.

It is essential that effective IM training be delivered to employees, because it promotes IM awareness and provides employees with the knowledge necessary to manage information throughout the information life cycle. The foundation to delivering effective IM training is a comprehensive IM training plan coupled with appropriate IM training, communication and awareness materials.

It is important that the overall approach to IM training be aligned with the Department’s IM strategy, while also addressing TB IM awareness and training requirements, to support efficient and effective training efforts. Through documentation review and interviews, auditors assessed the IMB Outreach Plan which includes details of the IM training and awareness activities planned for the 2013-14 fiscal year. A comparison of the IMB Outreach Plan against the Department’s IM strategy and relevant TB IM awareness and training requirements indicated that the IMB Outreach Plan was aligned with each. This alignment contributes to a solid foundation and structure for successful IM training delivery.

While having an adequate IM training plan is important, there should also be sufficient IM training, communication and awareness materials in place to enable the learning process. Auditors reviewed:

- IM training materials, including descriptions of in-person training, training presentation decks and Canada School of Public Service courses.
- IM awareness materials, including articles in the newsletter *This Week at IC*, email notices and Wiki posts.



Auditors performed an analysis that indicated the materials were offered at a frequency and through delivery media that promote effective IM practices. Auditors also reviewed a sample of IM training and awareness materials including the Employee IM Awareness Session and the Manager IM Awareness Session, and determined that the materials address attendees' needs, TB policies and departmental IM strategy.

By having the IM Outreach Plan and accompanying IM training and awareness materials in place to promote effective IM practices, the Department is well positioned to educate employees on leading IM practices and provide them with the knowledge required to effectively manage information through the information life cycle.

Results from the user survey indicated that the majority of employees understand IM policies, principles and record keeping best practices, specifically:

- 78% of survey respondents indicated that they understand the requirements for storing digital and paper-based information in accordance to the different security classifications.
- 73% of survey respondents indicated that they are aware of and understand IM policies, principles and record keeping best practices.

Additionally, although IM performance objectives and measures are optional in an employee's performance management agreement (EPMA), interviews and documentation review indicated that the IMB is promoting this practice through the weekly newsletter, *This Week at IC*.

Interviews with IMB and sector management indicated that there is a lack of awareness among the Department's employees of their IM roles and responsibilities. Of the survey respondents 73% stated that additional IM training would be beneficial to better fulfill their job responsibilities.

While the IM training, communication and awareness plan and materials are in place to promote effective IM practices, it is critical that employees throughout the Department receive adequate levels of IM training, retain IM knowledge and integrate leading IM practices into their daily operational tasks.

It is expected that employees throughout the Department receive adequate levels of IM training that allow them to perform leading IM practices in an efficient and effective manner. Of the 44 IM training materials identified, there were six mandatory IM training courses for those considered Information Management Functional Specialists, or those being promoted into Manager or EX roles. However, there were no mandatory IM training courses for all employees. Of the survey respondents 73% stated that additional IM training would be beneficial to better fulfil their job responsibilities.

More specifically, the lack of mandatory training creates a risk that employees do not have the required knowledge and skills on the basis of their education, training and/or experience to:

- Manage electronic records based on the IM life cycle and in accordance with Government of Canada IM policy.

- Classify and store sensitive information in accordance with Government of Canada IM policy.
- Fully comply with Government of Canada IM requirements.

Although 73% of survey respondents indicated that IM roles and responsibilities were communicated to them, interviews with IMB and sector management indicated that there is a lack of awareness among the Department's employees of their IM roles and responsibilities. Interviews with IMB and sector management also indicated that employees' lack understanding of potential impacts that IM activities can have on the Department.

There is a risk that employees lack a full understanding of how IM activities contribute to business performance, leading to missed opportunities to leverage IM to improve business performance.

Recommendation 5:

Employees should receive mandatory IM training on the following topics:

- IM roles and responsibilities
- The IM life cycle
- Information retention and disposition processes
- Classification of sensitive information

3.7 Management Response and Action Plan

The findings and recommendations of this audit were presented to CIO, IMB and Security Services CMS management. Management agreed with the findings included in this report and will take actions to address the recommendations both on an on-going basis and by Fall 2016 (planned completion of GCDOCS and the end of support for archived emails). The sectors and the CIO will share responsibilities for implementing the plan.

The CIO will ensure that all relevant strategies, policies and directives are updated, on a regular basis, to reflect the current government IM priorities and are communicated to all employees. The CIO will also complete the development of a recordkeeping performance framework with plans to expand the framework to cover all relevant information management activities. Through an IM Readiness Campaign that will support the Email Transformation Initiative and GCDOCS Project, the CIO and the Sectors will work together to review and update processes related to identification, file closing, retention and disposition of information and will ensure that these key processes are integrated with the functionality of new IM tools. Finally, the CIO in partnership with key stakeholders will deliver specific training on new IM tools; and will continue to provide IM Awareness sessions including the appropriate practices for classification and storage of sensitive information.



4.0 Overall Conclusion

The results of the audit revealed that, with exceptions, Industry Canada's IM governance and accountabilities are operating effectively to support the IM Agenda. However, improvements are required in the areas of IM processes, tools and training to fully support the achievement of the IM Agenda and enable compliance with relevant policies and directives.



Appendix A: Audit Criteria

Audit Criteria	Criteria Met / Met with Exception(s) / Not Met
IM Governance and Accountabilities	
1. Governance structures, roles, responsibilities and accountabilities for IM are defined and assigned throughout the Department.	Met
2. IM strategic planning is aligned with Department and GC priorities.	Met with exceptions
3. IM policy framework adheres to relevant GC legislative and policy requirements.	Met with exceptions
IM Processes and Tools	
4. IM life cycle requirements are incorporated in the Department's business processes and supported by departmental systems and tools.	Not met
IM Resource Capacity, Training and Culture	
5. Adequate IM training, communication and awareness initiatives are in place to promote effective IM practices, including document classification.	Met with exceptions