Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Audit of information management

Internal Audit and Program Evaluation Directorate

June 2025

Canada Border Services Agency

Agence des services frontaliers du Canada

ISBN 978-0-660-79465-5

Catalogue No. PS38-87/2025E-PDF

The Audit of information management is available on the Canada Border Services Agency website.

Aussi offert en français sous le titre : Vérification de la gestion de l’information

Audit of information management

Internal Audit and Program Evaluation Directorate
June 2025

Table of contents

Introduction

The Canada Border Services Agency (CBSA or the agency) ensures the security and prosperity of Canada by managing the access of people and goods to and from Canada. The information collected, generated, stored and used by the CBSA to deliver on its programs and services is significant, and much of it is sensitive in nature.

Information is a vital organizational asset that drives business decisions, while information management (IM) is a discipline that helps organizations achieve their business objectives by ensuring that information is reliable, accurate, complete and readily available, while also ensuring privacy protection.

The effective management of information is a foundational element of the Government of Canada's digital transformation. The Treasury Board *Policy on Service and Digital* requires that information and data be managed by the federal public service as a strategic asset under the leadership of departmental Chief Information Officers.

At the CBSA, the IM program was introduced around 2012. Early efforts focused on the roll-out and adoption of Apollo (the CBSA's version of GC Docs) as the agency's designated digital repository for business value information.

Despite the agency's demonstrable progress in adopting Apollo, recent public interest in CBSA procurement files, as well as past CBSA internal audits and reviews, have highlighted weaknesses in

fundamental IM lifecycle practices such as: not documenting key decisions for historical reference; information not being stored in corporate repositories or not being organized and labelled properly; and a lack of monitoring and oversight of IM activities and practices.

IM is essential to every facet of the CBSA's operations. It underpins informed decision-making, ensures efficient and effective service delivery, facilitates collaboration across organizations, and is a crucial factor to the achievement of the agency's objectives.

About the audit

The objective of this audit was to assess and determine the adequacy of the CBSA's IM framework, including monitoring and oversight activities, to support personnel in the consistent implementation of required and recommended digital IM lifecycle practices.

Audit scope inclusions

The scope period spanned April 1, 2023 to November 30, 2024, and centered on the IM framework and its implementation, as well as enterprise monitoring and oversight mechanisms. The audit focused on Apollo, as the agency's official corporate repository for digital records of business value.

Audit scope exclusions

The audit scope excluded the following:

- all information systems other than Apollo
- the CBSA's Data Strategy
- IM lifecycle practices for paper/physical records
- Information Technology infrastructure and system design and enterprise architecture, including business continuity plans
- structured data and operational systems
- risk of insider threats and data/information leaks
- testing of Information Technology general controls, such as network access and security controls
- quality of information for decision-making

Audit methodology

- 150+ documents reviewed
- 75+ stakeholders interviewed (including Information Administrators (IA) from 20 different areas of the agency)
- 300+ completed surveys
- 5 focus group sessions held with the manager community, with a total of 56 participants

Audit significance

The *Policy on Service and Digital* and supporting policy instruments serve as a set of rules on how Government of Canada organizations manage service delivery, information and data, information technology, and cyber security. The CBSA is a complex organization, with an equally complex IM landscape featuring dozens of information systems, a wide array of stakeholders, and a variety of IM needs across different teams, programs and operations. An effective IM framework and sound IM practices, aligned to TBS policies, are foundational to an organization's ability to leverage information for decision-making.

An IM compliance framework is specifically designed to ensure that an organization adheres to legal and regulatory requirements. With the ever-increasing volume of information and documentation, and the sensitive nature of information handled by the CBSA, a robust and well understood management framework for IM is vital in ensuring information assets are effectively and efficiently managed throughout their lifecycle.

Statement of conformance

This audit engagement conforms to the Treasury Board's *Policy* and *Directive on Internal Audit* and the Institute of Internal Auditors' (IIA) *International Professional Practices Framework*. Sufficient and appropriate evidence was gathered through various procedures to provide an audit level of assurance. The agency's internal audit function is independent and internal auditors performed their work with objectivity as defined by the IIA's *International Standards for the Professional Practice of Internal Auditing*.

Audit conclusion

An IM framework is fundamental in any organization where information is collected, produced, used or shared. It helps align the organization's IM practices with its strategic goals and priorities, as well as with applicable policies and instruments. Additionally, a carefully designed and implemented control framework provides for the effective management of information as a valuable corporate asset throughout its lifecycle, ensuring that legal and regulatory requirements are met.

The audit found that the CBSA has a low level of IM maturity and lacks the foundational elements of a robust control framework for IM, such as enterprise governance and oversight, IM plans and strategies, IM policy, and continuous improvement mechanisms. Further, while CBSA employees, managers and executives are generally aware of their IM responsibilities and have access to associated training and resources, the implementation of best practices is lacking. The absence of IM leadership and direction within individual teams, paired with the lack of practice monitoring and associated accountability mechanisms, may lead to a range of risks for the agency, some of which have already materialized.

With the recent creation of the Information and Management Systems group, the CBSA has a unique opportunity to bring renewed attention to the effective management of information, as well as to establish a rigorous control framework around it. This would help mature the agency's IM practices, both at the enterprise level and in employees' day-to-day activities.

Recommendations summary

1. Ensure CBSA employees have the necessary training and tools to effectively use Apollo (or the system of record to be adopted as Apollo's replacement) and apply good IM practices.
2. Ensure availability/completeness of relevant policies/procedures/instruments, and ensure awareness, particularly at the manager level.
3. Clarify roles and responsibilities for IM and opportunities to integrate IM practices in business processes.
4. Develop and implement monitoring and quality assurance mechanisms to support accountability in IM.
5. Define IM program objectives and refresh the IM strategy/plan accordingly.

Management response

The Vice President (VP) of Information and Management Systems (IMS) appreciates the audit's thorough assessment of the CBSA's current IM practices. IMS acknowledges the identified gaps, including system limitations and policy and process deficiencies, and has detailed plans to address them.

Importantly, as part of the Refocusing Government Spending initiative noted in the audit report, the CBSA is planning a migration away from Apollo to a Microsoft M365-based Enterprise Document and Records Management System. This transition will inform our response to the audit findings, as many of the identified issues will be addressed through the new system's design and implementation.

Information management is a collective responsibility that involves every employee within the Government of Canada. Effective IM requires the active participation and commitment of all employees, from senior leadership to frontline staff. IMS, in collaboration with key partners, is committed to addressing the challenges identified, and ensuring that the CBSA has a strong framework that enables IM excellence.

Our response is guided by our understanding of practical IM and acknowledges CBSA's accountability to address the challenges and leverage opportunities. Going forward, the Records and Information Management Strategic framework and associated management action plan deliverables will be designed to be practical and easy to implement, minimizing administrative burden and complexity.

Policy instruments and other deliverables will be developed through extensive consultation with stakeholders at all levels. This collaborative approach will ensure that diverse perspectives will be considered and integrated. IMS will engage in open and transparent dialogue throughout the development process and by fostering a culture of collaboration and mutual respect, we aim to build policy instruments, frameworks, communication products and standard practices that are not only effective but also widely supported and embraced by the entire organization.

We are committed to maintaining a dynamic and responsive approach to IM, where management excellence and employee input drives innovation and enhances our practices. This includes accountability mechanisms that will be established to monitor the implementation and effectiveness of IM practices.

Audit findings

The audit resulted in the findings below.

Information management policy framework and practices

A policy framework is a set of guidelines, standards and procedures that establish how an organization and its employees should conduct their activities. In the context of IM, a policy framework helps ensure that information is created, stored, shared and disposed of in a consistent and secure manner by providing direction on approved/recommended practices. Within the Government of Canada, IM is governed and guided by the *Policy* and *Directive on Service and Digital* and associated instruments.

CBSA IM Policy

There is an opportunity to strengthen the agency's direction on IM. While a CBSA IM Policy was published in 2020, it was removed from the agency's intranet in late 2024, due to not having been formally endorsed by senior management prior to its release.

Further, while Apollo was deemed the official corporate repository in 2018, messaging and language in CBSA policy/guidance has been inconsistent as to whether or not Apollo is in fact mandatory to use. For example, neither the former CBSA IM Policy, the intranet page on Apollo, nor the CBSA New Employee Orientation Tool and Guide explicitly indicate that the use of Apollo is mandatory. Based on survey results and consultations with various stakeholders, there appears to be a heavy reliance on Outlook and shared network drives to store business-value information, rather than Apollo.

Effectively, the onus is on business units to decide whether to use Apollo, and there is no process or standard governing this practice. Business units are not required to report centrally on the system of record they use for business value information. As a result, the agency has limited visibility into which groups do or do not use Apollo, and what is used in its place to store business-value information. This presents numerous risks, including potential loss or compromise of information, inefficiencies locating information, duplication of records, lack of information to support decision-making, compliance issues, etc.

Putting policy into practice

The effectiveness of a policy is determined by how well it is put into practice. Even a well-designed policy or procedure can fail if it is not properly executed, monitored or enforced. Several factors are essential in assuring policy objectives are met, including:

- providing associated training
- ensuring awareness of the policies/procedures
- integration of the corporate policies/procedures in daily operations
- having accountability measures, enabled by oversight mechanisms

To assess the implementation of IM best practices, challenges and root causes, the audit collected insights via an agency-wide survey, focus groups with the CBSA manager community, interviews with various stakeholders, and discovery testing in Apollo.

Information retention and disposal

As part of the agency's IM control framework, the CBSA's Retention and Disposition Schedules stipulate how long various types of documentation/information are to be retained, along with disposal procedures. Only 5 of the 20 groups consulted as part of this audit were aware of these documents, and some did not understand how they apply to their business unit. Instances were noted of information being disposed of without following the procedures defined by the Schedules. Risks associated to the lack of awareness around information retention and disposition include, for example, retention periods exceeding legislated authorities, and premature destruction or unauthorized disposal of business value information.

IM and project management

The CBSA's Project Management Framework sets direction for all agency projects. It briefly mentions IM and the use of Apollo but does not establish requirements such as where to store project documentation, or what to save in Apollo (governance decisions, project decisions, etc.).

The audit's cursory review of three major agency projects (CBSA Assessment and Revenue Management, Land Border Crossing, and Security Screening Automation) showed that business value documentation and project artefacts can be difficult to locate due to unclear document naming, complex folder structures, multiple document versions, no clearly identified final or signed copies, or documents simply not having been stored in Apollo. It was also noted that project decisions are often made via email but not saved in Apollo, and that governance decisions are not always documented in the projects' folders. As a result of these factors, tracing the history of the 3 sampled projects proved to be challenging[1]. This holds particularly true in instances where a project spans many years or where project team membership has experienced significant turnover, causing corporate and historical knowledge of the project to be lost.

IM roles, responsibilities and accountabilities

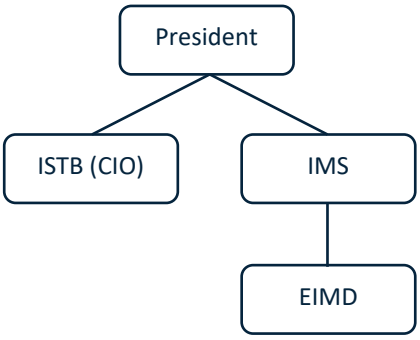
Clearly defined roles and accountabilities foster a sense of responsibility and ownership for IM, helping ensure that public servants at all levels understand what is expected of them in maintaining the quality, availability and protection of information they collect, produce, use or store.

Functional accountability

At the CBSA, the IM function previously resided in the Information, Science and Technology Branch (ISTB), whose VP is the agency's Chief Information Officer (CIO). In 2024, the function was carved out of ISTB and established as a stand-alone Information and Management Systems (IMS) group. The delineation of accountabilities and responsibilities between the VPs of IMS and ISTB (who retains the CIO title), and among their respective groups, has yet to be formalized. Further, though the Enterprise Information Management Directorate (EIMD) is the CBSA's functional lead for IM, program and

[1] As an example, in the case of the CBSA Assessment and Revenue Management project, an entire team was established by the Commercial and Trade branch to retrace and document the project's history, which required several months of work, research and follow-ups to locate missing documentation and information.

operational areas are responsible for adhering to policy instruments, adopting corporate direction and ensuring that their business processes are in alignment. This is neither defined, documented nor well understood among stakeholders.



What we heard:

- 78% of employees and 70% of managers believe they have a good understanding of their IM responsibilities. However, few managers could correctly identify their specific responsibilities. For example:
  - 41% were unaware they must ensure information assets remain available after an employee's departure from their team.
  - 34% were unaware that they must dispose of information according to the CBSA retention and disposition schedules.

Employees' roles and responsibilities

IM roles and responsibilities for agency employees, managers, other authorized users and IM Support are not fully formalized or well understood. While they were defined in the CBSA's 2020 IM Policy, the document was rescinded and has yet to be replaced. Though fragmented, some information is available on the CBSA's intranet and in the IM Roles and Responsibilities Grid for employees and managers.

As part of recent messaging by the CBSA's President on management excellence, there has been renewed communication on the importance of IM. Associated resources provided alongside the messages include guidance on managers' roles and responsibilities for IM.

IM training

Mandatory training at the CBSA includes a one-time course on Fundamentals of Information Management, as well as associated topics such as security awareness and privacy. Completion of these training modules is tracked by the agency, and managers are responsible for following up with their employees as required. While CBSA contractors were also required by the IM Policy to take these mandatory courses, completion is neither tracked nor enforced centrally. In light of IM challenges at the CBSA in recent years, the agency mandated all employees to re-take the Fundamentals of Information Management training in 2024. As of January 2025, completion rates across the agency had reached 88%.

Comments collected from stakeholders indicate that the mandatory IM training is too generic, and that there is a need for more targeted information sessions tailored to individual CBSA teams. This would foster discussion on how best to apply IM principles in a given operational context, and encourage teams to define their own IM procedures and requirements.

While IM training is mandatory, training on the use of Apollo is not, despite the fact that Apollo is the designated corporate repository for business-value information at the CBSA. Though Apollo Basics and Apollo Permissions training is available, survey results indicate that there is low uptake:

- 59% of regional respondents and 73% of headquarters respondents reported having taken Apollo Basics training
- 34% of regional respondents and 47% of headquarters respondents reported having taken Apollo Permissions training

Further, respondents indicated that a lack of knowledge and/or training and difficulties using the technology are some of the most important factors impeding good IM practices, signaling an opportunity to raise awareness as to what training is available, as well as to encourage greater participation in the sessions. Comments collected also indicate a need for more guidance and training material on IM roles and responsibilities and on Apollo functionalities, including job aids, cheat sheets, video clips on using key Apollo features, etc. Equipping employees with tools, guidance and resources is essential in enabling them to effectively use Apollo and apply good IM practices. This helps prevent risks and issues such as inadequate access control, security or privacy breaches, loss of information, etc.

Recommendation 1

The VP of IMS should ensure all CBSA employees have the necessary training and tools to apply good IM practices and use Apollo effectively (or the system of record to be adopted as Apollo's replacement).

Management response: Agree with forward-looking approach. IMS agrees that employees need appropriate training materials and practical tools to effectively use Apollo and apply good IM practices. IMS will focus on addressing immediate training needs while simultaneously developing a framework for learning, awareness and tools that will support both general IM practices and specific system functionality as we transition to our planned M365-based solution.

Completion date: March 2026

IM and Apollo resources

Though the CBSA's IM intranet page contains a variety of resources (including on roles and responsibilities, information retention/disposition, determining business value, document naming conventions, securing information, etc.), approximately 25% of survey respondents indicated that they were not aware of them. Further, only 35% of the business units consulted as part of this audit indicated having their own set of procedures to direct employees in applying good IM practices in the context of their operations.

While there are numerous examples of messaging in the CBSA Daily pertaining to IM best practices and resources, it was noted that such communications products may not always be read by, or resonate

with, employees. This underscores the importance of management communicating and emphasizing the need for good IM practices within their respective teams, providing direction, along with raising awareness as to the value of information assets and the risks associated with not managing them appropriately. Failure to do so may result in continued gaps in day-to-day IM practices, and continued risk exposure for the agency.

Recommendation 2

The VP of IMS should ensure relevant CBSA policies, procedures and/or associated instruments are up-to-date, readily available, and complete. Measures should also be taken to ensure greater awareness of this material, particularly among the manager community.

Consideration* should be given to the inclusion of formal direction on the mandatory use of Apollo (or its replacement) in CBSA IM guidance, as well as a requirement for the use of other repositories to be reported and approved by IMS.

*Considerations do not form part of the official recommendation but may be considered in the development of the associated Management Response and Action Plan.

Management response: Agree. Building off of the solid base of existing higher-level laws and policies[2], IMS will address specific gaps through targeted CBSA specific policy instruments while ensuring compliance is embedded in business process workflows.

Completion date: March 2026

Recommendation 3

The VP of IMS, in collaboration with program and operational areas, should clarify roles and responsibilities for IM and identify and pursue opportunities to better integrate IM practices in business processes.

Management response: Agree. IMS strongly supports a collaborative approach to IM. By working directly with business areas to embed IM practices within business processes and workflows, we will address the root causes of inconsistent information handling while creating sustainable improvements.

Completion date: June 2026

Daily implementation of IM best practices

Overall, input from stakeholders across the agency indicates that though employees, managers and executives generally understand their roles and responsibilities for IM, implementation is lacking. For instance, 79% of survey respondents reported having a good general understanding of the concept of business value information and their responsibility to appropriately save/store such information, but many feel that it is not always clear or easy to apply in their day-to-day role. This results in either excessive documentation being uploaded to Apollo unnecessarily, or documentation not being stored in

[2] Foundation Framework for Treasury Board Policies- Canada.ca

Apollo and residing only in email inboxes, personal drives or desktops. This leads to delays in retrieving information, or even to its loss.

Similarly, though CBSA employees at all levels are encouraged to email Apollo links instead of including file attachments, approximately half of the survey respondents indicated that they do not apply this principle. The use of Apollo links is also not possible when exchanging with the CBSA's external partners, who cannot access Apollo. The use of email attachments further exacerbates the potential for loss of documents or information, but also introduces challenges with version control, access control, etc. Several stakeholders acknowledged that business decisions are often made or recorded via email, but not subsequently uploaded to Apollo.

Most survey respondents indicated having a good understanding of the use of Apollo permissions. However, the audit's review of agency-wide Apollo folders surfaced thousands of documents for which access should have been restricted. These were mostly concentrated in one agency branch and one region[3]. Additionally, many respondents indicated they rely on the assumption that access to their teams' Apollo folders is restricted by default, which is not always the case.

In addition to the lack of knowledge/training and difficulties using IM technology, insufficient time was reported by survey and focus group respondents as the top impediment to good IM practices. Comments indicate that workloads, competing priorities and the fast pace of operations often result in IM becoming a secondary concern. Comments were collected from a wide range of stakeholders indicating that senior management (the EX-cadre) must better "walk the talk" and exemplify good IM practices. Among executive survey respondents, difficulties working with (or not knowing how to use) Apollo was reported as the primary factor impeding their ability to apply best practices.

Tone at the top

Recent messaging from the CBSA's President on management excellence has reiterated that IM is a fundamental responsibility of all employees and that, as such, it must be prioritized.

Accountability mechanisms

Holding agency employees accountable for performing good IM can involve various strategies. Among the most important are regular oversight by local management, integration of IM expectations in performance measures, and compliance monitoring by the CBSA's central IM function.

Focus group sessions held with the CBSA manager community indicates that there is minimal oversight performed of their respective groups' IM practices, with only 15% of respondents reporting that they regularly perform this type of activity. Paired with the reported lack of training/knowledge, challenges in using Apollo, lack of time, and the absence of IM procedures in individual groups, the absence of monitoring by local management presents significant opportunities for gaps in IM. This lack of

[3] Note that the audit team performed follow-ups with the document or folder owners to inform them of the issue and request that permissions be amended as appropriate. Examples of documents found include inland case management files detailing dates of birth (DOB), timeline of events, family details; detainee files including DOB, medical information; warrant files including DOB, inadmissibility information; electronic monitoring files including individuals' photographs, personal details and investigation information, etc.

monitoring/oversight at the day-to-day level can lead to unidentified and unaddressed IM issues, including the loss of business value information, privacy breaches, etc.

Additionally, only 31% of survey respondents were aware that IM was part of their annual performance measures. The remaining 69% reported that IM is not in their Performance Management Agreement, or that they were unaware if it is, further demonstrating that IM may not receive sufficient attention. These results align with comments indicating that there are no incentives to encourage good IM practices, nor compliance mechanisms to hold individuals accountable.

Compounded risk

Control gaps increase an organization's risk exposure. When there are several control weaknesses, the risks are compounded. As such, identifying and addressing control gaps promptly is vital.

In the context of the CBSA's IM program, the combined absence of a CBSA IM compliance framework, lack of understanding or application of associated roles and responsibilities, lack of business unit-specific procedures/requirements for IM, and the absence of day-to-day oversight of IM practices result in a significant opportunity for the loss of business value information, security or privacy breaches, and an array of operational and reputational damages for the agency.

IM is a shared responsibility among all CBSA teams and employees. While EIMD provides functional direction on IM, it is essential for individual teams to adopt the direction and ensure that it is understood, tailored and applied to their own operations. Regular monitoring is also key in ensuring that practices align with expectations.

IM and Apollo support

At the CBSA, there are two key groups providing IM-related support: the EIMD team and it's Apollo Support group, and Apollo IAs within the agency's various program and operational areas.

Audit consultations with stakeholders across the agency indicate a high level of satisfaction with services provided by the Apollo Support group. However, few indicated having engaged EIMD for advice and guidance on general IM practices.

Information administrators

In addition to the EIMD and Apollo Support teams, there are Apollo IAs across the agency, appointed by their respective teams as Apollo "super users." These individuals undergo dedicated training and are responsible for providing day-to-day support to their business units on the use of Apollo. The IA role is a secondary duty, and its application varies greatly from one group to another. While some IAs only provide the requisite Apollo support, others host IM information sessions, remind management teams of IM requirements and responsibilities, support employee onboarding with IM guidance, etc. Several IAs also noted that while they have sufficient capacity to respond to their teams' occasional requests for support, they do not have sufficient time to perform activities they believe would be valuable, such as conducting periodic "audits" of their teams' Apollo folders to ensure appropriate permissions are

applied, naming conventions are used, documents are stored in the right place, as well as to perform more coaching/providing information sessions, etc.

The number of IAs in a given team varies greatly; of groups consulted as part of this audit, the number ranged from 1 to 5 IAs per team. In larger teams with larger volumes of information and more intensive use of Apollo, having a single IA may not be sufficient. In consultations with regional 24/7 operations, it was noted that there should be enough IAs to ensure around-the-clock coverage, so that support can be provided in a timely manner. Similarly, comments indicate there should be at least one IA per port of entry or similar location, rather than one IA for an entire district, who may not be familiar with the intricacies of each team and their IM/Apollo needs. Further, survey results indicate a lack of awareness of the existence of IAs: 45% of regional respondents, and over 25% of HQ respondents indicated being unaware of IAs, or that they do not use these resources. Finally, while there is an intranet page listing IAs across the agency, the information is outdated. It was noted that IAs departing their teams are not always replaced and that the information is not always updated in the listing, which impedes the agency's ability to effectively leverage these resources.

Given the size of the agency, the complexity of its IM landscape and the EIMD's limitations, there is an opportunity to consider either expanding the IA role beyond purely Apollo support, or to explore the creation of an IM champion network, which could provide additional support, guidance, and accountability for IM across the organization.

Enterprise information management governance

An IM framework that includes clear expectations for governance and oversight is essential in ensuring that an organization's IM practices are aligned with strategic objectives. It provides a structured and comprehensive approach to managing information as a valuable corporate asset throughout its lifecycle, ensuring that it is effectively utilised and protected. It also provides direction for the organization's IM practices, which helps develop IM maturity.

Enterprise oversight

Governance and oversight provides a structured approach to decision-making, ensuring that decisions are well-informed and aligned with organizational goals, while mitigating risks.

Within the agency, the now-defunct CBSA Information Management Committee previously provided oversight of the IM program and practices. Currently, the DG Steering Committee is the only body in the CBSA governance structure that has a documented role in overseeing IM, though it is only one of its many areas of responsibility. Further, while an IM risk is documented in the agency's Enterprise Risk Profile, the extent of discussion on the topic cannot be ascertained based on the limited available records of committee discussions. Without an adequate level of enterprise oversight of the IM program, IM risks and issues may not receive sufficient senior management attention, or benefit from concerted commitment to improvements.

Enterprise monitoring

Monitoring mechanisms are essential in identifying risks, areas for improvement and ensuring compliance with application legislation and policies. It also enables an organization to collect pertinent information to assess the level of maturity of a program and the achievement of its objectives.

Proactive monitoring

From an enterprise IM standpoint, there is a CBSA National Management Reporting Framework; however, it is outdated (2016), not aligned with current Government of Canada and CBSA governance and strategies, and includes only very high level metrics which may not be meaningful, such as the number of Apollo users.

Additionally, an IM risk is recorded in the CBSA's Enterprise Risk Profile, for which the risk rating was elevated to "high" in 2023 to 2024. While planned risk mitigation activities and associated timelines were documented, progress has been limited and there has been no associated reporting. Consequently, IM-related risks and challenges may not receive sufficient attention from agency senior management, which may further impede or delay progress and mitigation plan implementation.

Issue/Incident Reporting

There are three main mechanisms for issue/incident reporting related to IM:

- EIMD's Apollo Support mailbox monitored by the Apollo Support Team. Common issues/concerns are followed upon via IA coaching calls, updated training content, and/or communications in the CBSA Daily or on Atlas.
- Security Incident Reporting and Preliminary Privacy Breach Reporting, managed by the Chief Security Officer (CSO) and the Chief Privacy Officer (CPO), respectively, whose monitoring and oversight responsibilities are documented in the CBSA Policy on Information Management Security. Reports include privacy breaches or disclosure of personal information, wrongful access/use of information, etc. The most common issues reported relate to inappropriate permission settings in Apollo, resulting in unauthorized access.
- Reporting of employee misconduct via a generic mailbox or CBSA's Internal Fraud Hotline monitored by the Professional Integrity Division. From 2022 to 2024, there were four allegations of misconduct relating to Apollo, all originating in a single region. This raises questions as to whether issues do not occur in other areas of the agency, or whether they are not being reported.

The CSO and CPO offices track, analyse and report on incidents/investigations in both internal and external reporting products, including the CBSA Administrative Investigations Annual Report and the Annual Report to Parliament on the Privacy Act. Recurrent issues, breaches and misconduct are communicated to management with recommendations for remedial actions; however, follow-up is limited and may result in gaps in controls remaining unaddressed. Finally, there appears to be limited sharing of pertinent information among the offices of the CSO, CPO and EIMD, which could support trend identification, improvements to the control framework, and other measures to mitigate risks in the future.

Recommendation 4

The VP of IMS should strengthen the enterprise IM oversight practices by developing and implementing an IM compliance framework that includes monitoring and quality assurance mechanisms at the enterprise and business process level, as well as accountability measures to incentivize good IM.

Management response: Agree. IMS agrees oversight and accountability is essential and will formalize the compliance function and establish a framework that will introduce monitoring and quality assurance mechanisms.

Completion date: June 2026

IM plan and strategy

A corporate strategy for IM is important to align practices with departmental objectives and provide direction for the program. This helps ensure that information is effectively managed, stored and utilized, and that clear expectations are set. Within the Government of Canada, the Information Management Guidelines outline the key elements of a standard IM plan and note that such documents should be developed or revised every 3 to 5 years.

The CBSA Five-Year Plan for IM came into effect in 2019. It contains no performance measures that would enable systematic monitoring of IM practices and challenges. No update on progress on this plan has been provided to agency governance bodies, nor has a new plan or strategy been developed or endorsed since. In the absence of an enterprise plan or strategy with associated performance metrics, timelines and resources, the agency's IM program may not be enabled to achieve measurable progress towards IM maturity, and existing enterprise risks may remain unaddressed.

Updates to the CBSA IM strategy and associated plans are particularly important in light of the significant changes that have taken place since 2019, including:

- separation of the IM function from ISTB in 2024
- nationalization of the program in 2020
- increasing reliance on digital document storage stemming from the pandemic and the shift to remote work
- increasing number of litigation holds
- heightened public and parliamentary scrutiny and associated need to easily and quickly retrieve information

All of these factors have resulted in a rapidly shifting IM landscape, and more change may be on the horizon: a proposal to move away from Apollo was tabled early in 2025 as part of Refocusing Government Spending efforts. Without a renewed IM Strategy, the CBSA opens itself to risks of misalignment with federal IM direction, continued inefficiencies in retrieving information, failure to manage information in compliance with applicable regulations, and missed opportunities to improve the agency's IM practices in a coordinated and cost effective manner.

Recommendation 5

The VP of IMS, in consultation with the CIO and other relevant stakeholders, should define the IM program objectives, performance measures and IMS mandate, and integrate this information and strategic direction in a revised and updated IM Strategy and plan.

Management response: Agree. IMS strongly agrees and has begun developing a modern IM strategy centered on a defined mandate, metrics and program objectives to address evolving IM needs and system-based requirements.

Completion date: March 2026

Appendix A: Audit criteria

Lines of enquiry	Audit criteria
1. Management framework	1.1 The agency has clearly defined and communicated roles, responsibilities, and accountabilities to support agency personnel in the consistent implementation of required and recommended digital IM lifecycle practices. 1.2 The agency's IM policies, procedures and guidance are up-to-date, sufficient, communicated, accessible, and are consistently implemented by all CBSA personnel. 1.3 The agency has an established IM plan and strategy, including performance measures and timelines to support agency personnel in the consistent implementation of required and recommended digital IM lifecycle practices. 1.4 The agency has an IM training path to support agency personnel in the consistent implementation of IM requirements and best practices.
2. Monitoring and reporting	2.1 The agency has monitoring and oversight mechanisms in place to assess and report on the implementation status of required and recommended digital IM lifecycle practices for Apollo by agency personnel. 2.2 The agency enables continuous improvement of Apollo IM practices by leveraging feedback mechanisms and implementing corrective action.

Appendix B: Audit survey

Information management is the responsibility of all employees of the agency.

The audit survey was available to all CBSA employees and executives and ran from November 8 to November 20, 2024. Participation was voluntary. The survey presented respondents with approximately 21 questions addressing:

- their IM and Apollo practices
- IM and Apollo challenges
- associated training and guidance

Of the 487 respondents, 301 fully completed the survey. Responses provided in partially completed surveys were used where applicable.

- The total 487 respondents included:
    - Executives: 13 (3%)
    - Employees: 365 (75%)
    - Managers/Supervisors: 83 (17%)
    - Apollo IAs: 26 (5%)

A note on survey biases

Internal audit recognizes that survey responses/results are susceptible to biases. As such, they may not provide a fully accurate representation of the agency's position on IM. However, results provide valuable indicators as to potential challenges and issues. Potential biases include the following:

- **Recall and social desirability biases**: For example, due to a few recent IM-related communications in the CBSA Daily, respondents may recall recommended IM practices and then answer accordingly as it is the desirable answer.
- **Non-response**: Occurs when survey participants are unwilling or unable to respond. These individuals can be systematically different from those who participate fully, thereby skewing the result. Examples of reasons for non-responses may include not being familiar or in compliance with IM practices, not using Apollo, lack of interest on the topic, etc.
- **Neutrality bias**: Finally, due to a few Not applicable or 'Other' responses without any comments provided in the survey or some Managers not commenting during the Focus Group sessions, these methods are subject to the neutrality bias in which persons avoid answering the question. These Not applicable or other responses were not taken into consideration in the audit's analysis.

Appendix C: Acronyms

CBSA	Canada Border Services Agency
CIO	Chief Information Officer
CPO	Chief Privacy Officer
CSO	Chief Security Officer
EIMD	Enterprise Information Management Division
IA	Information Administrator
IM	Information Management
IMS	Information and Management Systems
ISTB	Information, Science and Technology Branch
VP	Vice-President