Employment and Social Development Canada | Emploi et Développement social Canada

Canada

Audit of Information Sharing Agreements

Report

January 2025

Internal Audit and Enterprise Risk Management Branch

Audit of Information Sharing Agreements

Large print, braille, MP3 (audio), e-text and DAISY formats are available on demand by ordering online or calling 1 800 O-Canada (1-800-622-6232). If you use a teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. Em20-200/2025E-PDF
ISBN: 978-0-660-75042-2

1. Background

Employment and Social Development Canada (ESDC—the Department) manages an extensive number of programs and engages in extensive information sharing. The management of the Department's information holdings (including personal information) is a complex undertaking. Information is stored both physically and electronically across many systems, program areas, branches, and regional offices across the country. Information Sharing Agreements and Arrangements (ISAs) are records of understanding relating to personal information disclosed between parties[1]. ISAs are important for the Department to effectively manage information sharing with various stakeholders.

1.1 Audit Objectives

The objective of this audit was to provide assurance to senior management on:

- the extent to which ISAs are effectively managed; and,
- the extent that the ISA process is managed according to the relevant Treasury Board Secretariat (TBS) policy.

1.2 Scope

The scope of the audit included a comprehensive approach to ISA management, covering Information Sharing Agreements and Arrangements, Info Source (Information about Programs and Information Holdings), and other related items to the ISA process. All ISAs currently active for a given process or program were included within the scope. The audit did not assess or review previous ISA versions that have since been replaced with updated ISAs.

1.3 Methodology

The audit used the following methodologies:

- Documentation review and analysis;
- Data analysis and walkthroughs;
- Interviews with management and staff; and,
- File review.

2. Audit Findings

2.1 Roles and Responsibilities are not clearly defined, documented and delineated for all relevant stakeholders

The Departmental Policy on Privacy Management (DPPM) sets out responsibilities of departmental stakeholders for managing ISAs. While the DPPM mentions the role of the Chief Privacy Officer as the Department's functional authority on all privacy matters, which includes the provision of authoritative advice and functional direction to all ESDC branches and regions, it does not delineate Chief Data Officer Branch's (CDOB) role in the ISA process.

[1] Directive on Privacy Practices

Stakeholders have expressed confusion about the roles, responsibilities, and accountabilities of the Privacy Management Division (PMD)—overseen by the Chief Privacy Officer—and CDOB. Multiple stakeholders/branches highlighted uncertainty regarding the involvement of PMD and CDOB in various steps of ISA creation and management.

While CDOB expressed interest in developing ISA-related activities and initiatives over the next several years, there is currently no roadmap or detailed implementation plan.

Recommendation

1. PMD, in collaboration with CDOB, should update the departmental policy to define roles, responsibilities and accountabilities of all stakeholders for ISA management activities, monitoring and oversight.

Management Response

We agree with the recommendation.

PMD and CDOB will collaborate to develop new and update current departmental privacy policy and information management instruments, respectively, to clearly define the roles, responsibilities, and accountabilities of all ESDC stakeholders for ISA activities, including their development, approval, management, monitoring, and oversight. These complementary instruments will set out the roles of the Chief Privacy Officer, the Chief Data Officer, PMD, and CDOB in accordance with their respective authorities and mandates. New products and procedures will be developed to proactively communicate these parameters to stakeholders.

2.2 The current established guidance documents are not aligned with the new requirements per the TBS Directive on Privacy Practices and related guidance

The Department's standard ISA template used in the development of new ISAs (a key document for managing ISAs) was last updated in 2016. Since then, the TBS released a new ISA template in early 2023 and updated ISA guidance in mid-2023. PMD and CDOB have been developing an updated ISA template and guidance, but these updates are not yet complete. Consequently, the Department's current supporting guidance and templates do not yet align with the new TBS guidance.

PMD has gradually increased the level of ISA-related guidance provided to ISA program owners, which includes various presentations on the Department's intranet. However, there is a limited amount of targeted internal training specifically related to ISAs. Most interviewed ISA branch coordinators are unaware of the available ISA-related guidance material. Branches expressed strong interest in increased general (and targeted) training, which could help mitigate risks associated with information-exchange.

Recommendation

2. PMD should finalize updates to the departmental ISA template and guidance to align with the new TBS policy and guidance.

Management Response

We agree with the recommendation.

PMD and CDOB are collaborating on the development of new ISA templates and guidance documents that incorporate the 2023 TBS template and guidance. These instruments will comply with TBS's October 2024 privacy policy updates.

Further updates to ESDC ISA templates and guidance will be issued to ensure alignment with the planned ESDC privacy directive on ISAs and CDOB's Data and Information Sharing Governance Framework.

The new ISA requirements will be communicated to internal stakeholders and clients. PMD's ISA training products will be adapted, and new offerings, whether in-person or online, will be prepared and delivered with increased frequency or availability.

2.3 The Department maintains ISAs from various periods, of which many are not regularly reviewed nor updated, lack expiry dates, and lack key information such as details on methods of exchange

The TBS *Directive on Privacy Practices* and related guidance:

- defines ISAs as being "a written record of understanding that outlines the terms and conditions under which personal information is disclosed between parties";
- outlines that ISAs with appropriate safeguards should be established prior to any disclosure of personal information; and,
- provides information on areas ISAs should address (i.e. purpose of the ISA, retention/disposal of information, general safeguards, review periods, expiry dates, etc.).

It was observed that many of the Department's ISAs did not contain review periods, expiry dates or sufficient details on the method-of-exchange section.

Recent updates to the TBS *Directive on Privacy Practices* require each department to make available to the public summaries of all ISAs via an annual update to the institution's online "Info Source". There is risk that the Department may list expired (or inactive and no longer relevant) ISAs on the public Info Source.

Recommendation

3. PMD should create a plan to update ISAs to conform with TBS requirements and expedite updates of ISAs deemed to be of the highest risk.

Management Response

We agree with the recommendation.

PMD, in collaboration with CDOB, will review and conduct a risk assessment for each of the approximately 1,000 ISAs held in CDOB's repository. Privacy analysts will identify and assess any gaps with relevant privacy legislation as well as TBS and ESDC privacy policy requirements.

ISAs that are identified to be at a greater risk to privacy breaches will be prioritized and identified to their branch/program owners for updating. In situations where the ISAs can not be updated, branch/program owners will be required to prepare and implement risk management plans that are endorsed by the Chief Privacy Officer. PMD will provide oversight on the implementation of these plans and monitor the management of the agreements.

2.4 PMD and CDOB are not sufficiently monitoring ISA-related exchange activities and are not informing governance on the exchange activities

The ISA repository, established in 2016 and maintained by the CDOB, serves as the Department's primary tool for ISA management. CDOB is responsible for ensuring its completeness and ongoing maintenance. PMD limits its role to

activities directly related to the creation of ISA documents and does not actively participate in the management or execution of ISAs after they are finalized and signed by the program owner at the Assistant Deputy Minister level.

Most branch stakeholders interviewed found the ISA repository neither user-friendly nor particularly effective for managing ISAs. Furthermore, the Department lacks a detailed, consistent, and structured method to assess and rate ISA risk-levels, which impacts the ability to identify ISAs that may require additional scrutiny by the Data Privacy Committee (DPC).

Furthermore, a monitoring function for the information-exchange activities related to ISAs does not exist to confirm compliance with ISA requirements and adequate practices for safeguarding information transmission and access. Additionally, the DPC's oversight role in the ISA process is not defined in its Terms of Reference.

Recommendation

4. PMD should strengthen the approach to assessing ISA risk levels, undertake risk-based monitoring activities of ISAs to validate that information exchange practices are adequate, and periodically inform governance of results.

Management Response

We agree with the recommendation.

PMD has conducted risk assessment for ISAs that are less structured or formal than would normally be found for privacy impact assessments (PIA). It will implement a PIA process for ISAs that concern the use of personal information for administrative purposes and privacy protocol analyses that include risk assessments of ISAs that involve the non-administrative uses of personal information. Through these approaches, PMD will improve the structure, rigour, and consistency of the privacy risk assessment process for ISAs. The branch/program owner will be required to develop and implement risk management plans.

PMD, in collaboration with CDOB, will introduce a new ISA oversight program. PMD will collect information on the implementation and management for each ESDC ISA on a periodic basis to assess the privacy and agreement management controls and to determine whether any new risks have emerged that require mitigation. ISAs will be prioritized based on risk and through a random selection.

The results of these reviews will be presented to DPC for its consideration and to ESDC's senior leadership. DPC is mandated to provide oversight on risk management processes for department-controlled data and personal information, including monitoring risks, the implementation of risk mitigation strategies, and examining matters that could pose a significant risk to the Department.

Recommendation

5. CDOB, in collaboration with PMD, should develop an implementation plan for required enhancements to the ISA repository, as well as any additional planned improvements.

Management Response

We agree with the recommendation.

CDOB is currently working on the redesign of the ISA repository. Planning is underway to migrate it to a modern platform. The repository metadata is being reviewed and adjusted, where necessary, to support legal and policy compliance and improve decision-making. CDOB will work with PMD to optimize the repository to support the oversight and monitoring of ISAs.

3. Conclusion

In conclusion, the Department faces challenges in effectively managing ISAs in line with TBS requirements. Roles and responsibilities among stakeholders are not clearly defined, guidance documents are outdated, and many ISAs lack regular reviews, expiry dates, and essential details on data exchange methods. Furthermore, monitoring of ISA-related activities is not undertaken by the PMD or CDOB. Enhancing documentation, updating guidance, and strengthening oversight will be essential for improving compliance and data protection.

4. Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the Audit of Information Sharing Agreements. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

APPENDIX A: AUDIT CRITERIA ASSESSMENT

Audit Criteria	Rating
Roles and Responsibilities	Missing Key Control(s): Elevated Risk Exposure
Guidance and Support	Controlled but should be strengthened: Medium Risk Exposure
Agreements and Expertise	Missing Key Control(s): Elevated Risk Exposure
Management and Oversight	Controlled but should be strengthened: Medium Risk Exposure

APPENDIX B: GLOSSARY

CDOB	Chief Data Office Branch
DPPM	Departmental Policy on Privacy Management
DPC	Data & Privacy Committee
ESDC	Employment and Social Development Canada
ISA	Information Sharing Agreement/Arrangement
PIA	Privacy Impact Assessment
PMD	Privacy Management Division
TBS	Treasury Board Secretariat