Employment and Social Development Canada
Emploi et Développement social Canada

Canada

Unclassified

Audit of the Management and Implementation of Select Privacy Impact Assessments

June 2018

Internal Audit Services Branch

Audit of the Management and Implementation of Select Privacy Impact Assessments

This publication is available for download at canada.ca/publicentre-ESDC .
It is also available upon request in multiple formats (large print, MP3, Braille, audio CD, e-text CD, DAISY or accessible PDF), by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. : Em20-115/2018E-PDF
ISBN: 978-0-660-28395-1

ESDC
Cat. No. : SP-1191-11-18E

TABLE OF CONTENTS

1. BACKGROUND

1.1 Context

The Department creates, collects, retains, uses, discloses and disposes of personal information to deliver services to Canadians in a timely, accurate and secure manner while protecting confidentiality, integrity and availability.

The Department must comply with additional protection of personal information above and beyond the requirements of the *Privacy Act* as outlined in the *Department of Employment and Social Development Act*. This Act contains, for example, provisions for the exchange of information relative to Social Insurance Numbers.

As part of its Privacy Management Framework, the Department uses Privacy Impact Assessments (PIAs) to identify, assess and manage privacy risks for new or substantially modified programs or activities that require the creation, collection and handling of personal information.

PIA creation and management require close collaboration between program or activity areas, information technology (IT) security, departmental security and other departmental stakeholders such as privacy advisors and, when warranted, legal counsel. In certain cases, the Department has to coordinate the management of PIAs with other institutions.

Under the authority and direction of the Chief Privacy Officer (CPO), the Privacy Management Division (PMD) supports the Department in developing PIAs. The Division also supports the horizontal coordination and implementation of departmental strategic plans and priorities as it relates to the protection of privacy. The Division is responsible for privacy compliance and review services, privacy policy, strategic planning and coordination of privacy issues.

Once completed, PIAs are presented to the Privacy and Information Security Committee (PISC) and then forwarded to the Deputy Minister (DM) for approval. PIAs approved by the DM are submitted simultaneously to the Office of the Privacy Commissioner and the Treasury Board Secretariat of Canada's.

1.2 Audit Objective

The objective of this audit was to determine whether the current PIA approach results in the implementation of privacy practices that comply with legal and policy requirements.

1.3 Scope

The scope of this audit included key departmental structures, processes and practices pertaining to the management and implementation of select PIAs approved by the DM.

1.4 Methodology

The audit was conducted using a number of methodologies including:

- Documentation review and analysis;
- Interviews with management and staff from PMD;
- Interviews with management and staff from Branches as well as from Ontario and Québec regions; and
- Judgmental and risk-based sampling and review of 15 PIAs (see Appendix C for the list).

2. Audit Findings

2.1 Controls to achieve thorough identification and consistent assessment of privacy risks need strengthening

Treasury Board Directive on PIAs requires that once the need for an assessment is established, a PIA that contains the following must be completed:

- All elements of personal information collected and the manner in which they are collected;
- Where the personal information is stored, where it transits and who has access to it (i.e. information flow);
- An analysis of how the program or activity will comply with the *Privacy Act*;
- Risk identification and assessment; and
- Mitigating actions resulting from the risk identification and assessment in a manner that is commensurate with the risk identified.

Internal Audit reviewed a judgmental and risk-based sample of 15 PIAs approved by the DM in 2015–16 and 2016–17. All PIAs reviewed touched on the above components.

Internal Audit noticed a significant improvement in the quality of the PIAs approved in 2016–17, when compared to those approved in 2015–16. This improvement coincides with the introduction of the new PIA template. Risk identification was adequate for most of the PIAs reviewed. However, certain aspects of the privacy analysis were incomplete or incorrect and need strengthening. For example, 5 of the 10 PIAs that used the updated template did not address, as required, the encryption of personal information that is stored or in transit. Furthermore, information flow descriptions for 4 PIAs were either incomplete or did not reflect reality. This means that personal information is stored or transits by means unassessed by the PIA, the worst case being a PIA that did not identify nor assess the risk of sensitive personal information being sent from clients to the Department over the internet, in unencrypted emails.

Branches responsible for the administration of programs or activities covered by the PIA are tasked with creating PIAs. This decentralized approach has led to inconsistencies where similar risks have been assessed differently. For example, the use of Shared Services Canada's infrastructure has been assessed as a high risk in certain PIAs, an unknown risk in others, and some did not identify it as a risk.

Thorough identification and consistent assessment of privacy risks are key components of the development of adequate risk mitigation activities. PMD acts as a centre of expertise to assist Branches in the development of their PIAs. When a PIA has been identified as a priority by PMD, a PMD analyst is assigned to support Branch staff in the creation of the

PIA. However, through the years, PMD has been faced with staffing shortages that affected their capacity to provide timely and consistent advice. Also, when a PIA has not been identified as a priority, support from PMD is minimal, sometimes limited to providing the Branch with the PIA template.

Internal Audit notes that the Departmental Security Officer is responsible and accountable for physical security risk identification and assessment. The departmental IT Security Coordinator is responsible and accountable for IT security risk identification and assessment. However, the CPO is not responsible and accountable for privacy risk identification and assessment (as it currently resides within individual Branches).

Recommendation

1. The Department should assign to the CPO the responsibility and accountability to complete sound privacy analyses, thorough identification and consistent assessment of privacy risks found in the Department's PIAs.

Management Response

Management agrees. The Departmental Policy on Privacy Management assigns functional authority to the CPO. Under the direction of the CPO, PMD will do a review of the operationalization of this responsibility, including the accountability to complete sound privacy analysis through the identification and consistent assessment of privacy risks and report to Senior Leadership on possible improvements and clarifications to the current approach by January 2019.

As per its mandate, PISC has to oversee the development and review of PIAs. This can be viewed as a control to increase the consistency and quality of PIAs as well as an opportunity to facilitate the discussion on privacy risks and their acceptance by members of the committee. However, based on a review of PISC's records of decisions since June 2017, substitutes attended the majority of meetings for 11 of the 19 members. In addition, almost half of members (or their substitutes) were absent for 3 or more of the 11 meetings. PIAs were often provided to members two or three days before the meeting, which might be insufficient for members to provide meaningful comments and recommendations. This is illustrated by the fact that PIAs are almost always recommended for approval by PISC members. Internal Audit was informed that the committee's mandate may be revised in light of a review on data governance and management.

2.2 Senior management is seldom provided a comprehensive and integrated view of privacy and IT security risks

PIA creation and management require close collaboration between programs or activity areas, and IT security. The alignment and integration of IT risks with the protection of personal information was raised in the 2015 Audit of the Departmental Control Framework for the Management of Personal Information. The Department has reported that the IT security office was fully integrated into the PIA review process in April 2017. However, Internal Audit noted that 12 of the 15 PIAs reviewed identified potential risk exposure resulting from the absence of an IT security assessment. Uncompleted IT security assessments were sometimes ranked as a "medium" or "high" risk and sometimes labelled as "unknown".

Furthermore, privacy risks identified in IT security assessments were not always clearly portrayed in the corresponding PIA. For example, a PIA assessed the risk of using a particular system as low risk. However, the IT security assessment of that system identified four high risks to the confidentiality of personal information. None of these IT risks related to confidentiality had been fully mitigated when the PIA was approved and, as of April 2018, two were still outstanding.

Internal Audit also found that none of the 15 PIAs reviewed had been updated following the completion of relevant IT security assessments, even in cases where high risks to personal information were raised. For example, one PIA mentions that "in the event that risks have been identified [in the IT security assessment], they will be mitigated prior to the implementation of [the program]". However, despite two high risks and three medium risks to confidentiality identified in the IT security assessment, a statement of authorization was signed to approve an Authority to Operate with conditions (to allow time to satisfactorily mitigate risks identified in the assessment), which is at odds with the commitment made in the approved PIA.

Recommendation

2. The CPO should include privacy risks identified in IT security assessments in PIAs and monitor that they are mitigated with activities commensurate with the risk identified.

Management Response

Management agrees. PMD will ensure that IT security is consulted on every PIA and their advice is integrated into the analysis. PMD will also monitor IT security risks and work with IT security to ensure mitigation actions align with level of risk. Actions are expected to be completed by August 2018.

2.3 Controls to verify that the Department has implemented activities mitigating risks to privacy are missing

PIAs are intended to ensure that privacy implications will be appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented. Internal Audit identified 116 mitigation activities in the 15 PIAs reviewed. Our analysis indicates the following:

- Internal Audit believes recurring themes would benefit from being addressed in a more strategic or horizontal way. Such themes include: updating Personal Information Banks (for 11 of the 15 PIAs); defining retention schedule or a disposition authority (for 9 of the 15 PIAs); and, updating privacy notices to clients (for 8 of the 15 PIAs);
- 20 mitigation activities (17%) had no completion dates (12 to mitigate low risks, 3 to mitigate medium risks and 5 to mitigate high risks). Internal Audit questions the effectiveness of identifying no completion dates for a mitigation activity, especially if it addresses a high risk;
- 79 mitigation activities (68%) required collaboration with Branches other than the one signing off on the PIA. Furthermore, the diffused responsibility structure makes the timely implementation of mitigation activities challenging. Follow-up becomes more tedious and, in some instances, some Branches are responsible for carrying on mitigation activities for which they are not accountable; and
- 38 mitigation activities (33%) required a significant involvement from the Innovation, Information and Technology Branch (IITB); most of which relate to the completion of IT security assessments. Given current constraints, IITB has developed a separate work plan for the completion of security assessments based on risk. Senior management would benefit from being informed in the PIA itself that IITB has not included a system in their priority risk-based work plan. In those cases, it needs to be made clear that an IT risk assessment will not be conducted and that this constitutes a residual risk being accepted by the organization.

Internal Audit has also assessed the status of the 116 mitigation activities contained in the 15 PIA reviewed and has found the following (as of April 2018):

- The Department had accepted the risk for 18 of the activities reviewed. Internal Audit has concerns with 4 of those 18 risks: in some cases, the current mitigating mechanisms don't effectively reduce the privacy risks to an acceptable level. In another case, individually acceptable risks, when combined together, raise the compounded risk to a level that would, in our opinion, necessitate action;
- For 22 activities, the Branch responsible for the PIA could not provide a status on their implementation. The vast majority of those activities require collaboration between departmental Branches, with external partners or both;
- 42 activities were completed. Internal Audit deemed that, of these 42 activities, 33 had fully addressed their respective risks whereas 9 had only partially mitigated those risks (3 addressing high risks, 2 addressing medium risks);
- 18 activities were in progress, 13 of which had not identified a planned completion date (2 addressing high risks, 11 addressing medium risks, 4 addressing low risks and 1 for which the risk level was unknown);
- 11 activities were not started and did not identify a planned completion date (4 for medium risks, 6 for low risks and 1 for which the risk level was unknown); and
- The remaining five activities were considered obsolete and did not represent a concern to Internal Audit.

Considering the vast amount of time spent by Branches to produce PIAs, the Department needs better follow-up on the implementation of mitigation activities, especially for high and medium risk items. Centralizing the follow-up function could also lead to efficiency gains by preventing the duplication of follow-up activities by multiple Branches to internal service organisations such as IITB.

Recommendation

3. The CPO should be responsible for following-up on mitigation activities to verify if they are implemented as documented in the PIAs.

Management Response

Management agrees. PMD will develop a risk based approach to ensure appropriate follow-up and implementation of PIA action items is implemented.

As an interim step, PMD will begin a review of outstanding PIA action items on a pilot basis beginning in July 2018 with existing resources. An assessment of what further resources would be required to fully implement a refined approach will be reported to Senior Leadership by January 2019.

Internal Audit also visited two regions to see how PIAs with significant regional components had been implemented. Internal Audit found that personal information was adequately protected but discrepancies were noted between the theoretical environment described in the PIAs and actual operations. For example, risks associated with personal information being carried outside of government premises when performing on-site visits were not assessed in the PIAs. Risks associated with lost or misplacement of physical files by courier were also omitted in the PIAs. Use of information repositories undocumented in PIAs may also increase the risk of retaining information longer than required.

3. Conclusion

The audit concludes that the current PIA approach resulted in the implementation of privacy practices that mostly comply with legal and policy requirements. However, this approach does not rely on a sound control framework, it rather relies on whether officials implementing programs and activities involving personal information exercise due care.

The audit identified improvements in controls to achieve thorough identification and consistent assessment of risks to personal information. The audit also noted that the Department needs to follow-up on mitigation activities outlined in approved PIAs to confirm their implementation.

As the Department continues to enhance its Privacy Framework, roles and responsibilities need to be revised to identify privacy implications appropriately, assess them with consistency and resolve them adequately, before a new or substantially modified program or activity involving personal information is implemented.

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 management and implementation of the 15 PIAs reviewed in this audit. 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
It is expected that the Department has implemented controls to achieve:	Thorough identification of risks to personal information		Controlled, but should be strengthened; medium-risk exposure
	Consistent assessment of risks to personal information		Controlled, but should be strengthened; medium-risk exposure
	Adequate mitigation of risks to personal information	Identification of mitigating actions	Controlled, but should be strengthened; medium-risk exposure
		Follow-up on mitigating actions	Missing key controls; high-risk exposure
It is expected that the information presented to senior management supports sound decision making and careful consideration of privacy risks.			Controlled, but should be strengthened; medium-risk exposure
It is expected that the Department's risk assessment processes have been aligned and integrated to provide a comprehensive view of privacy, physical and IT security risks in a consistent and timely manner.			Controlled, but should be strengthened; medium-risk exposure
It is expected that the Department has put in operation privacy practices in compliance with legal and policy requirements for programs and activities involving personal information.			Controlled, but should be strengthened; medium-risk exposure

APPENDIX B: GLOSSARY

CPO	Chief Privacy Officer
DM	Deputy Minister
IITB	Innovation, Information and Technology Branch
IT	Information Technology
PIA	Privacy Impact Assessment
PISC	Privacy and Information Security Committee
PMD	Privacy Management Division

APPENDIX C: PRIVACY IMPACT ASSESSMENTS REVIEWED BY INTERNAL AUDIT

1. Canada Disability Savings Program: Administration of Canada Disability Savings Grant and Bonds
2. Temporary Foreign Worker Program, Phase IV
3. Compensation for Employers of Reservists Program
4. Workforce Development Agreement
5. Service Canada Role in International Mobility Program Inspections
6. Integrated Learning Management System
7. Interdepartmental Memorandum of Understanding on Collection Services with the Canada Revenue Agency
8. Federal Workers' Compensation under the *Government Employees Compensation Act*
9. Hootsuite: Hosted Social Media Account Management Service
10. Canada Apprentice Loans, Phase III: Repayment
11. Youth Employment Strategy
12. Individual Quality Feedback - Accuracy
13. Canada Education Savings Program Administration and the Delivery of the Canada Education Savings Grant, Canada Learning Bond and Provincial Education Savings Incentives
14. Passport Program Transition
15. Old Age Security Proactive Enrolment Initiative, Phase II