AUDIT REPORT OF THE PRIVACY COMMISSIONER OF CANADA

Assessing the Privacy Impacts of Programs, Plans, and Policies

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

The audit work reported here was conducted in accordance with the legislative mandate, policies, and practices of the Office of the Privacy Commissioner of Canada. These policies and practices embrace the auditing standards recommended by the Canadian Institute of Chartered Accountants.

This report is available on our Web site at www.privcom.gc.ca.

For copies of this report or other Office of the Privacy Commissioner publications, contact

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Telephone: (613) 995-8210, or 1-800-282-1376
Fax: (613) 947-8210
E-mail: publications@privcom.gc.ca

Ce document est également disponible en français

Table of Contents

Assessing the Privacy Impacts of Programs, Plans and Policies

Main Messages

1.1 It has been five years since the Policy on Privacy Impact Assessment (PIA) was first introduced by the federal government of Canada. Our audit found that some government institutions have made serious efforts to apply the directive, but that still more effort is required to ensure that the Policy is having its desired effect – that is, to promote awareness and understanding of the privacy implications associated with program and service delivery. While we did not identify any cases of pervasive non-compliance, generally speaking institutions are not fully meeting their commitments under the Policy. PIAs are not always conducted when they should be.

1.2 The extent to which privacy issues arising from government operations are appropriately managed is dependent on the maturity of the subject organization's PIA environment (specifically the management control framework in place to guide the evaluation of specific service delivery initiatives vis-à-vis an individual's privacy). While formal frameworks or administrative infrastructures have been introduced for most entities, these processes sometimes suffer from control weaknesses.

1.3 Despite the Policy's primary aim of ensuring that privacy protection is a key consideration in the initial framing of a project's objectives and activities, PIAs are frequently completed well after program implementation. In some instances, PIAs may not be completed at all (in spite of evidence of potential privacy issues emanating from program or service delivery). While privacy concerns are clearly emerging in the threat and risk analysis of new IT related projects, far less privacy consideration is provided for projects involving the inter-institutional and cross-jurisdictional flow of personal information.

1.4 Present PIA reporting and notification standards provide little assurance or information to Canadians seeking to understand the privacy implications of using government services or programs. Only a minority of government institutions regularly post and update the results of PIA reports to their external Web sites, and when summaries are posted, they often fail to disclose the privacy impact of new modes of delivery (and how associated issues are being resolved).

1.5 Although the application of Treasury Board directives encourages federal institutions to consider the privacy impacts of individual programs at the time at which they are conceived, the Policy, in and of itself, does not provide assurance that privacy impacts are being assessed for more pervasive and strategic government-wide initiatives. Knowing the potential privacy impacts of proposed policies and plans would provide Cabinet with an early opportunity to adjust or modify programs to protect the personal information of Canadians, and to reduce future costs associated with program changes.

1.6 To ensure the incremental effects resulting from the combined influences of various government institutions (or actions within a single department) are properly assessed, PIAs should consider the cumulative privacy effects that are likely to result from a program in combination with other projects or activities that have or will be carried out.

1.7 To ensure that the PIA Policy's original goals are being achieved, and to continue building trust with Canadians, now may be an opportune time to review the Policy. Policy renewal by the Treasury Board of Canada should include a review of the roles of the Treasury Board Secretariat (TBS) and the Office of the Privacy Commissioner of Canada (OPC), as well as the introduction of instruments that assist federal institutions in streamlining PIA activities and reports.

Background and other observations

1.8 The federal government has indicated that it is committed to both the protection of privacy in its own operations and to the general principles of fair information practices. According to the Treasury Board Secretariat, the government is "committed to protecting Canadians' personal information in the delivery of services across all channels...ensuring that privacy issues are addressed early in the design of services, that Canadians have confidence in the Government of Canada's handling of personal information, and that departments and agencies consistently adhere to the *Privacy Act* in the delivery of services."

1.9 In order to achieve these goals, the Government of Canada introduced its Privacy Impact Assessment Policy in May 2002. The Policy specifically requires that PIAs be conducted on all new initiatives that raise privacy risks and to share the results of that analysis (along with the measures proposed to address the risks identified) with the OPC for review and comment. The Policy further requires government institutions that have conducted PIAs to post a summary thereof on their external Web site.

The government has responded. The departments and agencies subject to this audit have generally agreed with our recommendations. Their responses, including the actions taken (or plans put in place) to address our recommendations, are set out within the audit report.

Introduction

The importance of privacy impact assessment

1.10 Public opinion surveys consistently demonstrate that Canadians are concerned about privacy when their personal information is used in the context of new or existing government services. As a recent poll demonstrated, a majority of Canadians agree that the protection of personal information will be one of the most important issues facing our country in the next ten years.

1.11 Potential privacy risks associated with government programs or services that rely on the use of personal information may include identity theft, inappropriate data matching or mining, and unintended disclosures. Privacy risks may also arise as a result of intra-institutional, inter-institutional, or cross-jurisdictional flows of information. The Privacy risks inherent in these activities need to be identified, assessed and resolved to ensure that the government respects the privacy of individuals. The *Privacy Impact Assessment Policy* is a key tool for meeting this challenge.

1.12 Privacy Impact Assessment (PIA) is a formal process that helps departments and agencies consider the effects of new programs or services (or proposed policies and plans) on the privacy of individuals. As a risk management tool, used in the planning phase of a program or service initiative, PIAs assist organizations to more fully reflect on the privacy implications of a given proposal, and may help reduce the costly redesign of programs, services, or processes.

1.13 The consequences of poor privacy insight were illustrated in the OPC's 1999-2000 Annual Report with respect to the planned *Longitudinal Labour Force File,* a massive information databank linking information from two federal departments along with provincial and territorial governments. The combination of huge personal databases, powerful computer systems, and growing links with provincial social programs and the private sector created significant privacy concerns. The government did not properly evaluate and mitigate such concerns, or anticipate the negative public reaction to the program, eventually led to the dismantling of the system at significant costs. Although this took place nearly eight years ago, and prior to the introduction of the PIA Policy, it reflects a groundbreaking moment for privacy protection within the federal government and a key example of the risks associated with poor privacy planning.

Tools for privacy integration

1.14 In May 2002 the Government of Canada introduced a policy on Privacy Impact Assessments. The Policy was adopted to assure Canadians that privacy principles would be taken into account when there are proposals for programs and services that raise privacy issues, throughout the design, implementation and evolution of those initiatives. The Policy prescribes the development and maintenance of Privacy Impact Assessments and requires government institutions to communicate the results of PIAs to the Privacy Commissioner and public.

1.15 At present, the privacy impact assessment process is the most comprehensive model in place to evaluate the effects of a specific service

delivery initiative on an individual's privacy, and therefore represents a core component of the federal government's privacy compliance regime. Although the assessment process was not intended for the development of new legislation, the Policy requires that institutions demonstrate that their collection, use and disclosure of personal information respects the *Privacy Act* (specifically Articles 4 through 8) as well as the ten privacy principles attached to the *Personal Information Protection and Electronic Documents Act*.

1.16 In addition to the government's Policy on PIAs, the Treasury Board Secretariat has issued *Privacy Impact Assessment Guidelines*, intended to help government institutions adapt the Policy to their own program and service requirements, while providing a general framework to manage privacy risks.

Privacy impact assessment and its place in the program life cycle

1.17 Combined with social, economic, environmental and other operational analyses, privacy impact assessment is intended to inform the decision making process that guides program and service delivery initiatives. It is an instrument that enables a decision maker to systematically analyze the privacy impacts of proposed programs, plans or policies. Applying the instrument rigorously will increase the likelihood of anticipating, preventing or mitigating negative privacy consequences, or in enhancing the positive impacts associated with the use of personal information.

1.18 Under the PIA Policy, institutions are required to initiate and define the scope of a Privacy Impact Assessment in the early stages of the design or re-design of a program or service so as to influence that program or service's development. But privacy impact assessment does not end after project design; it is intended to be an iterative process that is maintained throughout the life cycle of government initiatives. The end product of a PIA is the assurance that all privacy issues have been identified and resolved.

Federal responsibilities in applying the Policy

1.19 Ministers for departments, and other heads of institutions as designated by Order in Council, are responsible for ensuring that their organizations comply with the *Privacy Act, Regulations* and associated policies. The Privacy Impact Assessment Policy applies to all government institutions listed in the Schedule to the Act. It states:

> Deputy Ministers and other deputy heads of institutions are responsible for…determining whether initiatives have a potential impact on the privacy of Canadians and warrant the development of Privacy Impact Assessments, and for integrating and balancing privacy with other legislative and policy requirements.

1.20 Within government institutions, the responsibility for developing and maintaining PIAs is often shared between program and project managers, privacy policy experts, legal advisors, and functional specialists. Access to Information and Privacy (ATIP) divisions within institutions often play a critical role in the initiation, review and approval of PIAs.

1.21 As an Officer of Parliament, the Privacy Commissioner of Canada has the authority under the *Privacy Act* to examine the collection, use, disclosure, retention and disposal of personal information by government institutions

subject to the Act. Under the PIA Policy, the OPC is to receive notification of all Privacy Impact Assessments, and may provide advice and guidance to institutions with respect to potential privacy risks.

1.22 The Treasury Board Secretariat is responsible for interpreting the Policy, for providing advice to institutions, and for monitoring compliance. Institutions seeking preliminary project approval and funding must include the results of a PIA in their submission or project brief. TBS analysts are assigned to each institution and they may request that a PIA be completed if, in their view, one is required.

2002 Treasury Board Secretariat Policy Statements on Privacy Impact Assessment

On May 2, 2002, the Treasury Board of Canada Secretariat issued its Privacy Impact Assessment Policy. Although the Policy itself has not been substantially revised since its introduction, annual federal reporting requirements have been updated from time to time, most recently in 2006. Following are the 2002 Policy Statements on Privacy Impact Assessment.

Policy Statements

The Government of Canada is committed to protecting the personal information of Canadians. Privacy, in conjunction with other relevant legislative and policy considerations, is integral to the design, implementation and evolution of all programs and services. Although often associated with electronic service delivery, Privacy Impact Assessments provide a consistent framework to determine privacy risks inherent in any service delivery channel, including in-person, mail, telephone and on-line services.

Institutions are responsible for demonstrating that their collection, use and disclosure of personal information respect the *Privacy Act* and privacy principles throughout the initiation, analysis, design, development, implementation and post-implementation review phases of their program and service delivery activities.

Institutions are also responsible for communicating with Canadians why their personal information is being collected and how it will be used and disclosed. They must explain the impact of new modes of program and service delivery on privacy and how associated issues will be resolved. The result will be that Canadians can make informed choices regarding the type of service delivery channel they wish to rely on in their relations with the federal government and will be assured that their privacy is being protected regardless of the channel they choose.

Therefore, it is the policy of the government to:

- ensure that privacy protection is a core consideration in the initial framing of program or service objectives and in all subsequent activities;
- ensure that accountability for privacy issues is clearly incorporated into the duties of program managers and any other participants, including those from other institutions, jurisdictions and sectors;
- provide decision-makers with the information necessary to make fully-informed policy, program, system design and procurement decisions based on an understanding of the privacy implications and risks and the options available for avoiding and/or mitigating those risks;
- reduce the risk of having to terminate or substantially modify a program or service after its implementation to comply with privacy requirements;
- provide documentation on the business processes and flow of personal information for use and review by departmental and agency staff and to serve as the basis for consultations with clients, the Privacy Commissioner and other stakeholders; and
- promote an awareness of sound privacy practices associated with program and service delivery by informing the Privacy Commissioner and the public of all proposals for new or modified programs and services that raise privacy issues.

[The complete text of the Privacy Impact Assessment Policy can be found on the Treasury Board Secretariat's Web site at: http://www.tbs-sct.gc.ca]

Past reviews

1.23 In June 2004, the TBS commissioned an independent mid-year review of a limited sample of departments to determine the impact of PIA Policy in promoting privacy best practices. While remarking that there was evidence that the Policy was having the desired effect of improving compliance with privacy legislation, the study also identified several problem areas requiring attention, including:

- A lack of expertise in government and industry in the conduct of Privacy Impact Assessments;
- Difficulties in coordinating and integrating the contributions of stakeholders within departments;
- Challenges in harmonizing PIAs with other government of Canada policies, such as the government's security, data matching, and Social Insurance Number (SIN) policies;
- Delays in making PIA summaries publicly available; and
- The inability of departments to support PIA observations with documented evidence.

1.24 The study also remarked that there was no single reliable source of information on how many PIAs have been conducted, and that there appeared to be no mechanism in place to ensure that PIAs or preliminary PIAs (PPIA) were being conducted when warranted. Finally the study remarked that there was evidence that departments have not been properly monitoring the implementation of risk mitigating measures identified through the PIA process.

Focus of the audit

1.25 The principle focus of this audit was to evaluate the federal government's privacy impact assessment practices, including compliance with the requirements and goals of the TBS Policy on PIAs, and by extension, adherence to the *Privacy Act* and fair personal information management principles. We assessed the following nine institutions against four primary criteria (see **About the Audit** at the end of this audit report):

- Canada Revenue Agency
- Citizenship and Immigration Canada
- Correctional Service Canada
- Health Canada
- Human Resources and Social Development Canada (HRSDC)
- Indian and Northern Affairs Canada
- Royal Canadian Mounted Police (RCMP)
- Services Canada (an initiative of HRSDC)
- Veterans' Affairs Canada

1.26 In addition to the detailed audit work conducted on these nine entities, we conducted a survey of 47 additional institutions subject to the Policy and to the *Privacy Act*, asking each to self-assess against the same four evaluation criteria used in our primary review.

1.27 We also looked at the roles and responsibilities of two federal organizations with cross-departmental responsibilities – the Treasury Board Secretariat and the Privy Council Office – and those of our own Office.

1.28 Although the results of our audit are, for the most part, presented in aggregate, we have identified several examples of good practices in privacy impact assessment to highlight potential areas of practice improvement in departments and agencies. For more information about our audit objectives, scope, approach and criteria, see **About the Audit** at the end of this report.

Observations

Policy's application far from complete

1.29 Our audit found that federal institutions have generally been slow in implementing the Policy. Although we did not identify instances of pervasive non-compliance in any one department (or government wide), government institutions are not, by and large, fully meeting their commitments under the directive. In spirit, the privacy impact assessment process seeks to ensure that privacy matters are considered at program conception or design and that risks identified are mitigated prior to program implementation. In reality however, the Policy's application is far from complete.

1.30 In assessing a department's PIA practices, including its overall compliance with the government's PIA Policy, we focused our enquiries along the main responsibilities of institutions vis-à-vis the Policy and Guidelines, namely:

- To conduct PIAs, at the time of program or service design, for all new initiatives (or substantially redesigned programs and services) that may raise privacy risk;
- To provide a copy of the final PIA, approved by the Deputy Head, to the Office of the Privacy Commissioner, prior to implementing the initiative, program or service;
- To develop risk assessment and mitigating measures for privacy issues identified and to ensure that privacy mitigating measures are implemented; and
- To make PIA summaries public.

Additional details on this approach, and how departments and agencies were selected, are contained in **About the Audit** at the end of the report.

Implementation of necessary management frameworks is mixed

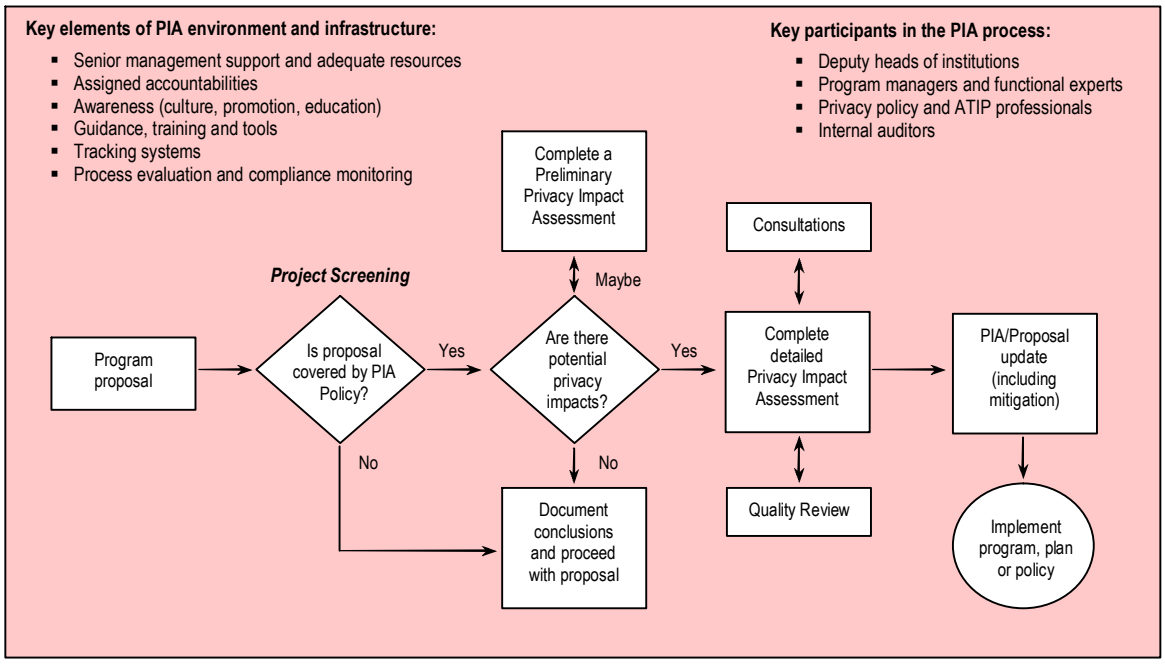
1.31 How an organization deals with the privacy issues arising from its operations is often influenced by the management systems the entity has in place to guide the evaluation of specific service delivery initiatives vis-à-vis an individual's privacy. Departmental compliance with the government's Policy on PIAs presupposes the existence of some administrative infrastructure to support the Policy's objectives and requirements. The absence of any such framework – or control deficiencies within such a process where one exists – is likely to have a direct and measurable impact on the effectiveness and quality of privacy impact assessments, and on the extent to which each entity is Policy compliant.

1.32 As departments and agencies are expected to comply with the Policy, deputy heads are ultimately accountable for ensuring that required systems are put into place. Key elements of a sound infrastructure should include, among others, evidence of:

- Programs in place to inform staff and other stakeholders of the Policy's objectives and requirements;
- Formally defined program responsibilities and accountabilities;
- The existence of a system to effectively report all new initiatives that may require a PIA/PPIA;
- The existence of a body composed of senior personnel charged with reviewing and approving PIA/PPIA candidates;
- The existence of an effective system of compliance monitoring; and
- Adequate resources committed to support the department's obligations under the Policy.

Exhibit A provides the outline of a generic system for conducting privacy impact assessments.

Exhibit A: Generic process (with key elements) for conducting privacy impact assessments



1.33 Although the OPC has observed a marked improvement in the quality and completeness of PIA submissions since the early days of the Policy's implementation, PIA and PPIA submissions that the Office now receives continue to suffer from common omissions and defects in documentation and analysis (see **Completeness of assessments varies but improving**). Although the reasons for such omissions and defects vary by organization, we believe that many are the product of process related weaknesses (i.e., deficiencies in the

administrative architecture supporting the PIA Policy at the departmental level) and a lack of PIA resource capacity.

1.34 In order to establish a reasonable benchmark for the evaluation of management control frameworks, the OPC developed a PIA Process Maturity Model. This model – derived from the control objectives for information and related technology (COBIT) and validated against the objective attributes of an effective management control framework described in paragraph 1.32 – identifies five progressive maturity levels, ranking each organization according to its standardization of processes. The model, illustrated in Exhibit C, can be used not only in measuring the maturity of each entity's PIA environment, but also as an indicator of the degree to which each entity is likely to be policy compliant.

1.35 **PIA environments are still maturing.** Of the nine entities we examined as part of our detailed audit activities, only three entities had what we would describe as well managed and measurable PIA environments (level 4). In contrast, four of the nine entities examined had PIA processes that we would consider largely *ad hoc* or recognized but intuitive (levels 1 and 2). This is surprising given that the PIA Policy has now been formally in place for five years, and that the entities in question oversee programs with substantial personal information handling requirements. The remaining two entities best fit into category 3, defined PIA process, having formally introduced PIA guidelines into their overall operations, but lacking adequate controls and oversight.

1.36 The results of our detailed audit work are consistent with the information we collected as part of our survey. Of the 47 federal institutions polled, 89% of respondents indicated that they were active in the use of personal information in the delivery of programs and services. When asked if the organization had a formal management framework in place to support the conduct of PIAs, a full 68% of respondents said no. More specifically, 29% of respondents self-assessed at level 1 (initial/ad hoc) on the PIA Process Maturity Model, and 54% self-assessed at level 2 (recognized but intuitive). Only one organization within our sample is said to have a fully optimized PIA process (i.e., level 5 on the PIA Maturity Model).

1.37 Exhibit B provides a point-in-time illustration of PIA environments across government based on the combined results of our survey and audit. Although we believe these results to be a close approximation of the state of affairs across federal institutions, the illustration was not intended to be statistically or scientifically representative of all organizations subject to the *Privacy Act*.

Exhibit B: Federal PIA Process Maturity versus normal distribution curve

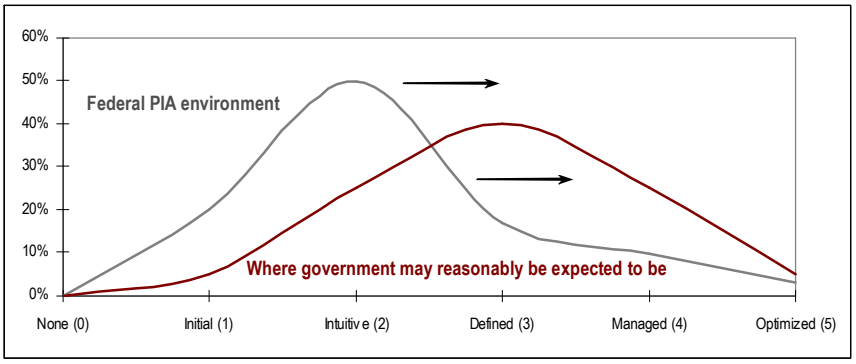


Exhibit C: Privacy Impact Assessment Process Maturity Model

The PIA process maturity levels of organizations we audited varied on account of multiple factors, the most notable influences being: organizational culture, human resources (specifically those dedicated to privacy policy); and the presence or absence of internal oversight. Generally speaking, organizations with strong cultures of confidentiality and an entrenched awareness of privacy issues were more likely to have mature processes for managing the conduct of PIAs. In contrast, those organizations with less sensitivity to the protection of personal information tended to have less mature PIA processes. Likewise, entities which had been subject to past audit, inspection, or public scrutiny were also more likely to have conducted internal reviews of their PIA infrastructure aimed at process amelioration.

Maturity Level	Status of the PIA Environment
0 Non-existent	There is no recognition of the need for Privacy Impact Assessments (PIAs). Privacy (including proper personal information handling practices more generally), is not part of the organization's culture. There is a high risk of non-compliance with the Policy and a high likelihood of privacy deficiencies or incidents. In such an environment, few, if any, PIAs are completed when required.
1 Initial/*ad hoc*	There is some recognition of the government policy and the need for an administrative infrastructure to manage the PIA process within the organization. The entity's approach to meeting Policy requirements is *ad hoc* and disorganized, and lacks formal leadership, guidance or monitoring by senior management. Deficiencies in the manner in which PIAs are conducted have not been considered or identified. Employees are not aware of their responsibilities within the organization or with respect to the PIA Policy government-wide. In such an environment, some PIAs are likely completed, but many are not, and the quality of privacy impact analysis is likely poor.
2 Recognized but intuitive	A PIA framework is in place but lacks critical elements to support the Policy's objectives and requirements. Control weaknesses exist within the PIA process and have not been adequately identified or addressed by Management; the impact of such deficiencies may be significant. Management may or may not be aware of their obligations under the Policy. Employees may not be aware of their responsibilities within the PIA process. The quality of PIAs and the manner in which a PIA is completed (including whether or not a PIA is initiated) is dependent on the knowledge and motivation of individual employees.
3 Defined PIA process	A formal PIA process is in place and documented. Management is fully aware of their PIA obligations and has begun introducing PIA guidelines into their overall operations. However, the process is not adequately enforced and there are some remaining control weaknesses within the PIA process. While management is able to deal predictably with most privacy issues which arise from operations, some control weaknesses persist within the PIA process and impacts could still be severe. Employees are aware of their responsibilities but the organization lacks adequate resources to support the department's obligations under the Policy.
4 Managed and measurable	A formal PIA process is in place and documented. Management is fully aware of their PIA obligations and is meeting their requirements and obligations under the Policy. Responsibilities/accountabilities under the Policy have been formally defined and both management and employees are proactively involved in all aspects of the PIA process. Programs are in place to inform staff and other stakeholders of the Policy's objectives and requirements and adequate resources have been committed to support the department's obligations under the Policy. An effective system of reporting of all new initiatives requiring a PIA/PPIA exists. For the most part, high quality PIAs are completed, when required, in a timely manner.
5 Optimized	The assessment of operational privacy impacts has been integrated into the entity's overall risk management framework (at the center of which exists a formal PIA process). Organization wide controls ensure continuous and effective monitoring for compliance with the organization's own PIA process and the Treasury Board Policy. An individual/body is charged with overseeing compliance with the Policy and a body composed of senior personnel is charged with reviewing and approving PIA/PPIA candidates once complete. The organization conducts performance monitoring on key financial, operational and human resource aspects of PIA operations, and the results of PIAs are integrated into ongoing project management.

1.38 Privacy impact assessment is not well integrated with operations. Across our sample of entities, the PIA process was far from being fully integrated into the overall risk management strategies of individual entities (though more formal linkages with key program centers, most notably information technology, appear to be emerging).

Privacy impact assessment practices vary

1.39 Amongst entities with relatively well defined PIA environments, we observed one of two recurring approaches to privacy impact management. In the first case (what may be referred to as the *Active ATIP* model), privacy or PIA experts within the entity's access to information and privacy unit (ATIP) act as promoters, educators, advocates, and ultimately the compliance authority within the privacy impact assessment process. In the second case (the *Passive ATIP* model), the role of ATIP is restricted to that of a consultant, who offers advice and guidance only when requested to do so. In the latter model, all control over the initiation and completion of PIAs rests with program managers (a wholly appropriate design where such managers are accountable for program delivery).

1.40 Although there appear to be operational advantages to each approach, the Active ATIP model seems to have had much more success in bringing about a general awareness of Policy requirements and in eliciting the support of senior management for PIAs. In many cases, the Passive ATIP model was characterized by the absence of dedicated policy professionals for privacy matters, leading to the underresourcing of PIA responsibilities in favour of those relating to access to information requests (a legislated vs. policy requirement).

1.41 Since enforcing compliance with the Policy calls for competencies beyond those of the ATIP shop of most government institutions, it seems natural that responsibilities within the PIA process remain shared. However, the responsibilities of each group should be clearly defined, well understood, and properly enforced – an important role for senior management.

1.42 Given the unique nature of most federal institutions and the differences in program and operational structures among them, it would be difficult to develop or implement any one common model or single administrative framework that would best support the PIA Policy. PIA models should generally reflect the nature of each institution's operations, incorporating the core control elements noted in Exhibit A, and remaining scaleable for resource limitations.

Some departments' frameworks are lacking critical control elements

1.43 Inadequate project screening may undermine Policy. The most common control weakness identified within the management systems we reviewed was the lack of a mandatory and formal screening process (for all programs, services, plans and policies) to identify potential PIA and PPIA candidates. Indeed, 64% of respondents we surveyed indicated that they did not have policies or processes in place to identify all activities requiring privacy impact analysis.

1.44 The absence of such a screening process – in essence, the trigger point for any privacy impact analysis – precludes an entity from properly assessing the extent to which there may be privacy risks associated with a proposal, and effectively contributes to instances of PIA omission. Absent a formal

mechanism to evaluate PIA requirements, government institutions may also be able to circumvent the government's policy requirements, deliberately or otherwise, without serious consequence.

1.45 Currently, a Treasury Board Submission is required to authorize or amend terms and conditions of programs governing grants or contributions, to recommend approval of Orders in Council that have resource or management implications, and to carry out a project or initiative, the costs of which would exceed a department's delegated authority. A Treasury Board Submission is an official document submitted by a Minister on behalf of her or his department to seek approval or authority from Treasury Board to carry out a proposal that the government institution would not otherwise be able to undertake (or which is outside its delegated authorities). As part of the standard Treasury Board Submission, government institutions are required to consider the need for a PIA, and to provide the final report prior to funding.

1.46 Although the PIA requirements associated with a Submission help to ensure that major, or soon-to-be-funded, proposals do not proceed without consideration of potential privacy impacts, the Submission process does not provide sufficient coverage over program changes or the various micro-initiatives undertaken within large approved programs. These smaller initiatives or program changes, particularly when combined, can have serious privacy impacts, and should therefore be given consideration as potential PIA candidates.

1.47 While the PIA requisites linked to project funding remain a critical external control in enforcing privacy analysis for project proposals, more effective "screening" calls for the fuller integration of privacy impact assessment into each government institution's operational and program planning. Given the inherent complexities of assessing the need for privacy impact assessment, project screening should be viewed as a process in and of itself rather than any one single administrative duty.

1.48 Some of the critical control components within a screening process might include: ongoing employee awareness programs, embedded administrative linkages between privacy analysis with other risk mitigation tools (e.g., IT threat and risk assessments or business case documents), or the institution of cross-functional authorities (e.g., privacy policy or ATIP) for program approval.

1.49 The use of a centralized tracking system for programs involving the use of personal information may further assist in monitoring PIA activities department-wide, and in assessing whether or not the institution has correctly identified all PIA or preliminary PIA candidates.

Gaps in coverage and delays in completing assessments

1.50 **Tracking systems are largely deficient.** We were unable to measure the full extent to which Privacy Impact Assessments across government had not been completed when needed, since most federal departments do not have adequate systems in place to monitor instances where PIAs are (or were) required.

1.51 Over the course of our audit, many institutions began introducing such applications and/or gathering the baseline data required to populate such a system. We believe that developing a comprehensive program inventory, while

both time and resource intensive, would yield important information regarding potential PIA omissions and serve as a beacon for potential privacy risks associated with programs already in place.

1.52 Despite the absence of hard statistical data on PIA omissions, there is sufficient anecdotal evidence to believe that the number of potential omissions is not substantial in comparison to the total number of government initiatives involving personal information, and that instances of omission have declined considerably since the introduction of management control frameworks for PIAs within government institutions. The Treasury Board Submission process provides some assurance that large or extraordinary projects would have been subject to privacy consideration prior to project funding.

1.53 **Program changes may create privacy risks.** If there is an exception to this trend however, it most likely lies within program or service delivery changes, where the internally defined requirements for PIAs are unclear and where PIA practices remain mostly unmonitored. Although the TBS Policy and corresponding Guidelines document provide broad directives on when institutions must initiate a PIA, the guidance can be difficult to interpret in the context of program changes, in particular those affecting existing IT systems.

1.54 **Information sharing may create privacy risks.** In addition to the privacy concerns emerging into the threat and risk analysis of IT related projects, little privacy consideration is provided for projects involving the intra-institutional, inter-institutional or cross-jurisdictional flow of personal information. In many such cases, accountability for privacy impact assessment rests with more than one institution, and responsibilities under the Act are seen to be limited rather than shared. Although the Policy clearly states the need to conduct a PIA in situations where programs or services are contracted out or devolved to another organization, there is no clear requirement for doing so in cases of information sharing (an activity governed by related data matching and data protection policies).

1.55 As departmental programs and initiatives become increasingly integrated, and as data sharing activities within government become more commonplace, the risk of privacy breaches or improper personal information handling practices increases accordingly. Currently, there appears to be a lack of policy guidance on the issue of PIAs where multiple organizations, portfolios, programs and/or jurisdictions are concerned. Memoranda of understanding (MOU) between organizations, while helpful in defining the terms of information sharing arrangements, do not necessarily ensure that all privacy risks associated with information sharing are fully mitigated. In several cases we observed, interdepartmental MOUs for information sharing were long outdated and did not provide adequate protection against potential privacy breaches.

1.56 Exhibit D speaks to the nature of select PIA omissions we identified over the course of our review. The underlying causes contributing to these omissions (as well as other related performance issues) are discussed in greater detail later in our report (see **Main Factors Contributing to Performance Gap**).

1.57 **PIAs are sometimes completed after the fact.** Equally as important as the issue of PIA omissions, is the point in time at which PIAs are initiated for projects with known or anticipated privacy risks. Over the course of our audit we noted numerous cases where PIAs were not initiated until well after a project's conception or design. While in rare cases, such delays were based on

the absence of information required to conduct the PIA, more often the delays in privacy impact assessment were unrelated to challenges in gathering data.

Exhibit D: The nature of Privacy Impact Assessment omissions

The following are case illustrations of potential or known PIA omissions identified over the course of our audit. They serve to highlight practice areas within government where additional effort is required to ensure the protection of personal information.

- **System changes**

Significant changes to the business processes or systems that affect the separation of personal information or the security measures used to manage and control access to personal information *may* create privacy risks. The automation of systems with personal information holdings that were previously paper based is one such example. System changes may also involve the expansion of personal information collection for purposes of program integration or eligibility, or the development of common personal identifiers for administrative purposes. Conducting privacy impact assessment on system changes during the early stages of system re-design is an effective way to ensure that privacy considerations are influencing the development process.

- **Programs introduced before the policy came into effect**

Although the Policy provides for an effective date of May 2002, it was drafted within the spirit of strengthening privacy protection in the delivery of all government programs and services, regardless of when those initiatives were introduced. Privacy Impact Assessments provide the framework for documenting the privacy risks inherent in all program activities and can be used to examine programs already in place. This is no less important than when considering the cumulative privacy effects of programs and services. Systems or service delivery initiatives created prior to May 2002 must be in compliance with the law. Consequently, Privacy Impact Assessments should be conducted to better understand the associated privacy implications and to ensure that programs are in compliance with the Act.

- **Sharing personal information**

Data matching activities, or the sharing of personal information between programs, institutions or jurisdictions, should always be subject to privacy impact assessment. Only through detailed analysis can an organization fully appreciate the risks and liabilities associated with such activities and the precautionary measures which should be adopted to mitigate identified risks. Although the *Privacy Act* only applies to federal institutions, most provincial and territorial governments are subject to similar privacy laws and policies that regulate the collection, use and disclosure of personal information. PIAs can assist in identifying the requirements of the various legislations and ensure that the provisions of federal legislation and policies are respected. Memoranda of understanding between organizations, while helpful in defining the terms of information sharing arrangements, do not necessarily ensure that all privacy risks associated with information sharing are fully mitigated or that privacy protections are periodically reviewed and enforced.

- **Pilot programs**

Program feasibility studies, run in a secure test environment or using fictitious data, may not be subject to the requirements of the PIA Policy. But to the extent that an organization plans on eventually using real data, in any live version of that program, Privacy Impact Assessments should be conducted, ideally at the same time as program design. Any initiative involving the use of real data, that of an identifiable individual, in even a limited manner (say regionally) or as a trial run (internally deemed as a pilot or prototype), requires a PIA and should conform to the *Privacy Act*.

- **Looking beyond electronic service delivery initiatives**

In ensuring that privacy considerations play a central role in guiding program and service delivery initiatives, there is perhaps no greater instrument available to program managers than education. Creating a general awareness of the policy requirements respecting privacy is often the first step towards ensuring that program managers fully consider the privacy impacts of their plans and priorities at the time of that initiative's conception. While the privacy risks of implementing electronic service delivery are increasingly recognizable, there may be privacy risks associated with other program activities, including: public consultations, research, and policy development, among others.

1.58 In several institutions we noted instances where Privacy Impact Assessments had not been conducted until well after a project's full

implementation. Although the Policy encourages privacy analysis to be conducted throughout a program's lifecycle, the absence of *any* such analysis prior to program implementation could aptly be characterized as a case of omission (particularly given the spirit in which the Policy was drafted). This is potentially problematic, not only in light of the Policy's original objective of building privacy considerations into the core of new programs, but given the high possibility of privacy breaches absent any detailed impact analysis.

1.59 **Substance over form.** It is imperative to note here that while our audit examined the timeliness with which PIA reports were completed vis-à-vis a project's implementation date, this measure may put unintended emphasis on the reporting component of privacy impact assessment, rather than on the *process* itself as a risk management tool.

1.60 While ideally a PIA would be used as a tool to guide program development, in our view, a PIA report that is issued soon after a project's implementation, and which adequately explains how all privacy risks were identified and mitigated, is likely better than a report which is produced "in time" but which fails to do the same. Unfortunately, since privacy impact assessment is an activity that is conducted over extended periods of time, it was difficult to assess when such analysis had begun for initiatives under review. Notwithstanding the imperfection of this audit measure, the observations noted above still hold true and are worthy of serious consideration.

Completeness of assessments varies but improving

1.61 In our 2005-2006 Annual Report to Parliament, we were pleased to note that many of the PIAs we had received were increasingly precise and thorough in their analysis (as compared to those submitted when the Policy was first introduced). Despite the notable progress considerable room remains for improvement.

1.62 Although there are often similarities between projects in the types of privacy risks encountered (and the general practices for risk mitigation), given the diversity of these projects it is important for PIAs to make recommendations specific to the type of information being collected and the types of systems being used. While generic statements concerning the accountability for protecting personal information are helpful in understanding the managing principles that will guide future actions, they are difficult to fully evaluate for follow-up and effectiveness. The OPC prefers to see a much more specific and proactive approach to mitigating privacy risks, and has recommended the issuance of binding guidelines, protocols and well documented procedures.

1.63 Similarly, PIAs submitted historically have not included guidance for privacy breach notification (i.e., the process institutions would follow to inform affected individuals if personal information has been found to be inappropriately disclosed). We continue to recommend that every institution have clear policies and processes in place to guide staff in instances where personal information has gone astray and may be at risk.

1.64 Finally, some PIA submissions continue to lack detailed action plans for the implementation of privacy protection strategies. These strategies are important in helping the OPC fully understand the manner in which identified privacy risks are to be addressed and in ensuring accountability for future risk mitigation.

Identified privacy issues slow to be addressed

1.65 As part of our audit, we sought to examine the extent to which the risk mitigation plans of departments (and the recommendations of the Office of the Privacy Commissioner) for a sample of PIAs completed over the past five years had been implemented. The results of our work, which may or may not be representative of PIAs across government, indicate that institutions are generally slow in addressing the identified privacy risks associated with programs and services.

1.66 Although the majority of "high risk" issues in our sample appeared to be addressed prior to program implementation (or in a reasonable time period thereafter where PIAs are completed post project implementation), a substantial number of issues, qualified by departments as "medium risk", remain outstanding up to, and in some cases more than, a year after programs are put into place. Some issues marked "high risk" remain similarly outstanding, and the progress in addressing such matters was deemed, by us, to be unsatisfactory at the time of our review.

1.67 Without underestimating the magnitude and complexity of certain initiatives, or the fact that some recommendations require significant time and investment to fully address, institutions did not appear to be actively monitoring the implementation of PIA observations, in some cases exposing themselves (and their clientele) to potential risk.

Poor public reporting and disclosure of privacy risks

1.68 Under the existing Policy, institutions must provide a copy of all final Privacy Impact Assessments to the Privacy Commissioner. This notification must occur at a reasonably early stage, prior to implementing the initiative, program or service. The advance notification is intended to permit the Commissioner to review the issues and, if appropriate, to provide advice to the head of the institution. To complement this requirement, and to promote a broader understanding of how privacy issues related to the program or service have been addressed, institutions must make summaries of the results of their Privacy Impact Assessments available to the public in a timely manner.

1.69 Given the nature of the PIA process as one that is relatively discreet and self-managed, the notification and public disclosure requirements of the Policy remain important instruments of accountability both to the policy centre and the general public.

1.70 Our audit revealed that, in some cases, PIAs are not submitted to the Commissioner in a manner which would allow for the provision of advice, if any, to the heads of institutions prior to program or service implementation. The absence of timely notification has a significant impact on the intended monitoring and compliance regime for PIAs government-wide.

1.71 To this end, it would be disingenuous of us not to recognize the effects of PIA service delays at the Office of the Privacy Commissioner. Although the Treasury Board Secretariat suggests a delivery standard of six weeks for the OPC to review PIAs submitted, currently the Office is providing comments, in many cases, some 18 months after a submission is received. These delays are due to resource limitations. While the PIA Policy was introduced in May 2002, the PIA review function at the OPC was not funded until 2006 (and for the two

years prior had only one full-time employee working on PIA reviews). At the time of writing this report, the OPC was in the process of hiring three PIA review officers and had engaged the services of professionals under contract to reduce the back log of pending reports. The Office currently employs a risk based approach to PIA reviews, expediting the review process for projects considered to be particularly privacy sensitive.

1.72 **Information in annual reports is insufficient.** Beyond the aforementioned OPC notification requirements, federal institutions are required to demonstrate that their collection, use and disclosure of personal information respects the *Privacy Act*. This is accomplished, in part, through public reporting mechanisms such as *Info Source* and the *Annual Reports on the Access to Information and Privacy Acts*. Although these reports were designed to ensure active and continuous monitoring of PIA activities, the reporting scorecard for Privacy Impact Assessments is limited to only three simple data points: the number of PIAs initiated during the year; the number of PIAs completed during the year; and the number of PIAs submitted to the OPC for review. These simple statistical summaries do little to strengthen public reporting and accountability, and do not appear to provide sufficient information for TBS to properly execute its stewardship and monitoring role.

1.73 **Poor information undermines public participation.** As previously mentioned, in order to promote a broader understanding of how privacy issues related to the program or service have been addressed, institutions must make summaries of the results of their Privacy Impact Assessments available to the public in a timely manner. At the time that our audit began however, only a minority of institutions were regularly posting and updating the results of PIA reports to their external Web sites. Of the nine entities subjected to in-depth audit, only four had made PIA summaries publicly available. In all but one of those four cases the inventory of summaries available on-line was incomplete.

1.74 Similarly, of the 47 federal institutions we surveyed, only 25% of respondents were said to be making PIA summaries accessible to the public through postings to their external Web sites. 50% of respondents indicated that PIA summaries were not being published at all.

1.75 Taking into account the fact that there may be components within individual PIAs that must be protected under the *Access to Information Act* or the *Privacy Act*, or that in certain cases, assessments contain information that would render systems or security measures vulnerable, one must question whether the current public disclosure standards are providing any value or comfort to a citizen seeking to understand the privacy implications of using a specific government service or program.

1.76 **Quality of PIA summaries reviewed was poor.** While Treasury Board recommends that the summary results of PIAs assume the form of an executive summary – elucidating the privacy impacts of new modes of program or service delivery, and disclosing measures taken to mitigate risks – none of the departmental summaries we reviewed on-line contained more than a project description and a simple conclusion or disclaimer along the lines of "…essential privacy requirements have been addressed and an action plan to further strengthen the privacy of Canadians has been adopted." Unsure as to whether such a summary was acceptable under the Policy, we compared a sample of departmental summaries with those of the Treasury Board Secretariat itself and found departmental summaries seriously wanting.

Good practices identified

1.77 Good practices exist in some federal departments. Some departments have developed the necessary processes to fully implement the Policy and are actively conducting Privacy Impact Assessments where required. We found good examples of governance, project screening mechanisms, guidance and training regimes, and cultural awareness programs in some of the departments and agencies we assessed (see Exhibit E).

1.78 Overall, one department – Human Resources and Social Development Canada (including their Service Canada initiative) – stood out among its peers. The organization benefits from a strategic Privacy Management Framework (which provides an overarching infrastructure to manage personal information and privacy) and a well structured PIA process. Since the Policy's introduction in 2002, these organizations have developed comprehensive guidance to supplement the TBS directives, introduced tools to help program managers conduct PIAs, maintained an active awareness campaign, and developed a process to appropriately identify and screen potential PIA and PPIA candidates.

Exhibit E: Good practices in privacy impact assessment

Privacy awareness • Citizenship and Immigration Canada

The Public Rights Directorate at Citizenship and Immigration takes up every opportunity to tell the privacy story. It has fostered the creation of an "ATIP Coordinators Network", a basic subject matter communications forum established with designated ATIP persons in each departmental branch. In addition to the monthly reports posted on the department's on-line ATIP/Privacy space, the Directorate holds an annual ATIP coordinators conference or retreat, bringing together privacy officers from headquarters and regional offices for workshops and discussions built around an agenda responsive to the declared needs of participants. Senior management awareness is fostered by frequent presentations to the Departmental Management Committee.

Strategic Planning and Governance • Human Resources and Social Development Canada

The department's Privacy Management Framework (PMF) was developed in late 2000 as a strategic starting point for the management of the organization's personal information holdings. The PMF, linked to the department's strategic planning and governance initiatives, examines the operational, administrative and research uses of personal information to ensure that all privacy issues are identified and mitigated through a collection of interrelated guidelines, best practices and tools (including the PIA). A Privacy Management Framework Committee is responsible for directing the enterprise-wide implementation of the Privacy Management Framework, both across and within departmental programs. The Committee meets monthly, and its membership consists of directors general, information and privacy coordinators, heads of internal audit as well as representatives of legal services and regions. Privacy Impact Assessments are reviewed and approved by the committee prior to their submission for Deputy Minister signature.

Project Screening • Royal Canadian Mounted Police

The CIO Sector at RCMP Headquarters in Ottawa has implemented a system of controls to assist in the screening of new or modified IT systems for potential privacy impacts. Effectively acting as gatekeeper for the conception and implementation of new projects, the CIO Sector assigns a project manager to oversee all development activities. The gating process is founded on a series of incremental screening criteria requiring executive level approval from a Project Review Board in order for a project to progress through to completion. Three of the screening gates address PIAs and contain provisions requiring project manager approval, consultation with the business owner, and ATIP (privacy) review. Projects that do not have required approvals are considered "out of bounds" and cannot proceed. While the CIO Sector responsibility is currently limited to national systems, those systems represent the vast majority of IT processes under the jurisdiction of the RCMP. Discussions are underway to adopt similar procedures at the regional level.

Guidance and Training • Health Canada

Creating a general awareness of the policy requirements respecting privacy is often the first step towards ensuring that program managers fully consider the privacy impacts of their plans and priorities at the time of an initiative's conception. Health Canada's newly introduced training regime for privacy and Privacy Impact Assessments offers a step by step introduction to the core concepts of fair personal information handling practices, communicates departmental responsibilities and accountabilities, integrates privacy principles with the larger Policy requirements regarding PIAs, and introduces important and practical privacy tools for program managers. The training suite also allows program managers attending the course to walk through and work on the development of a PIA for actual operational projects planned or underway.

Recommendations

Main factors contributing to performance gap

1.79 Although the Government of Canada's PIA Policy is beginning to have the desired effect of promoting awareness and understanding of the privacy implications associated with program and service delivery, five years after the Policy was first issued, we would have expected departments to be further along in supporting the initiative. Overall, there are varying degrees of commitment to the Policy. For example, some institutions have well entrenched PIA infrastructures, while others have only just begun to develop the basic systems required to support the PIA process. Based on our audit work, we believe that there are a number of main factors that have contributed to this performance gap.

Lack of management support and infrastructure

1.80 We would have expected senior management to have more clearly conveyed their commitment to the Policy, firstly by broadly communicating the importance of privacy protection in the delivery of programs and services, and secondly by formally articulating the expected outcomes of privacy impact assessment. We also would have expected the organization to have dedicated sufficient resources and personnel to address policy requirements, and to ensure that the commitments and expected outcomes of the Policy had been met.

1.81 Access to information and privacy officials play an important role in advising senior management of their obligations under the Policy. They also play a critical role in shaping and supporting the PIA processes within their respective organizations. In some federal institutions however, we noted that senior management had not been formally briefed by ATIP on PIA requirements since the Policy was first introduced in 2002. Although we could not measure the extent to which efforts to create a PIA infrastructure had been met with resistance by senior management, it follows that without senior management support, such an infrastructure would be difficult to create and sustain.

1.82 Beyond having the necessary resource capacity to fully implement the Policy, the single most important determinant in ensuring the successful evaluation of specific service delivery initiatives vis-à-vis an individual's privacy is the existence of a sound management control framework. The absence of such a framework is likely to have a direct and measurable impact on the effectiveness and quality of privacy impact assessments, and on the extent to which each entity is Policy compliant.

1.83 Recommendation: The deputy heads of all government institutions subject to the Policy should reaffirm their commitment to privacy protection and ensure that their organization is fully implementing TBS directives. They should ensure that their organization has introduced an adequate administrative infrastructure to support the conduct of PIAs and committed the necessary resources to ensure its application. This administrative infrastructure should:

- Identify and document all proposals that may present privacy risks;
- Establish a sound structure for organizational accountability;
- Develop and implement a system to track all proposals subject to the Policy, and the detailed PIAs conducted;
- Provide internal guidance and training to managers and staff who are involved in the preparation and leadership of programs, plans and policies; and
- Establish quality control, consultation, communication, follow-up, and evaluation procedures for PIAs.

Treasury Board Secretariat (TBS) Response:

TBS is fully committed to supporting institutions in achieving compliance with both the *Privacy Act* and the related privacy policy requirements. To this end, TBS will ensure that institutions have the necessary policy guidance and tools for achieving and implementing sound privacy management practices and complying with the requirements of the Act. In addition, specific requirements related to compliance with the *Privacy Act* and its policies will continue to be assessed as part of the Management Accountability Framework exercise.

Limited integration into decision making and assessment of effects

1.84 Government institutions often view PIAs as a separate, stand-alone obligation, rather than as a specialized risk management tool. As such, privacy impact assessment has yet to be fully integrated with other strategic planning instruments influencing the development of programs, plans and policies.

1.85 The timing of, and rigour with which PIAs are sometimes conducted suggests that some institutions view privacy as a mere afterthought to program and service delivery. Notwithstanding other considerations, drafting a PIA several years after a project's implementation suggests that a department may only be conducting the review in order to satisfy policy obligations (rather than using privacy analysis to influence a program's development). This is perhaps especially true when the findings from PIAs are slow to be addressed, and in those instances where PIAs are not completed for proposals with potential privacy impacts. While we appreciate that it is sometimes difficult to conduct an in-depth privacy impact assessment when the specifics of a program have yet to be developed, this was not a key contributing factor towards the cases of PIA omission and delay we identified.

1.86 Recommendation: Federal institutions subject to the PIA Policy should seek to better integrate privacy analysis, including the need for PIAs, into their overall approach to risk management by linking existing PIA Policy requirements with program activities and their respective administrative processes. Senior management should use privacy impact assessment, in

conjunction with other social and economic analyses, to influence the subsequent development of programs, services, plans and policies.

Treasury Board Secretariat (TBS) Response:

As part of its review of the existing privacy policy suite, TBS is currently exploring options for ensuring the integration of privacy analysis within broader institutional priorities and responsibilities. TBS's privacy policy will work to align PIA requirements with existing legislative responsibilities in order to reduce duplication of effort and streamline the privacy impact assessment process. Currently, the Management Accountability Framework exercise provides a measurement of privacy within a broad management context and TBS intends to build on this process.

Resources are stretched

1.87 In light of the maturity levels of institutional frameworks for managing PIAs, it was not surprising to learn that none of the institutions we audited had yet developed integrated financial, human resource or operational performance reporting measures for PIAs. Outside of contract and consulting expenditures, the full costs of conducting PIAs were generally not well defined, but instead recorded as part of 'corporate overhead'.

1.88 **Limited resource management.** While the costs associated with ATIP units within institutions were generally known and managed, product-type costing is not employed for PIA or privacy specific activities. This general lack of resource management may have a profound effect on the quality of PIAs, as institutions currently do not appear capable of properly assessing whether or not PIA resources are sufficient to fulfill their requirements under the Policy.

1.89 Given the causal relationship between resource investment and production quality, the under-funding of ATIP shops, specifically for PIA activities (vis-à-vis those related to access to information), appears to be particularly problematic. As PIAs become more entrenched in the overall risk management practices of departments, we would expect the associated costs to be more closely monitored.

1.90 **There is a shortage of privacy professionals in government.** Notwithstanding the lack of performance measurement for PIAs, our experience suggests that, in the case of privacy policy, and in particular privacy impact assessment, there is a shortage of qualified resources across government. We believe this shortage of privacy professionals is having a serious impact on the success of the Policy's implementation.

1.91 Almost without exception, we were struck by how few full-time personnel were dedicated to privacy policy and PIA initiatives. Generally speaking, institutions we audited had staffing complements ranging from 11,000 to 44,000 full time equivalents (with ATIP divisions employing 37 to 78 personnel). Within these same institutions however, privacy policy or PIA personnel numbered in the range of only 2 to 14. By any account, even when one considers the role that legal counsel, program managers and technical experts play in privacy protection, the total human resource base available for Privacy Impact Assessments in government is severely stretched.

1.92 Shortages in privacy resources are not limited to line departments and agencies. In the context of Privacy Impact Assessments, it is the Office of the Privacy Commissioner's role to review PIA submissions from all of government and to provide comments, if considered necessary, prior to program or service implementation. At the time of our audit, the OPC had only one full-time PIA Review Officer and a back-log of submissions dating nearly two years in arrears. The Office is currently in the process of re-building its audit and review capacity with the aim of working in a more timely and collaborative manner with federal institutions on PIAs (see also paragraph 1.71).

1.93 As a result of the shortage of PIA personnel, government institutions are relying heavily on the professional services of external contractors. Although the quality of contracted work is generally adequate, privacy impact assessment requires a sound understanding of business processes and data flows unique to each organization. In many cases, that knowledge resides exclusively with program and ATIP officials. By contracting out PIAs, institutions are less likely to develop the in-house capacity to conduct such assessments, and may overlook some of the privacy risks associated with plans or programs which could only be identified through introspection or self-review.

1.94 **Recommendation:** Federal institutions subject to the PIA Policy should assess whether or not present resources are sufficient to fulfill their requirements under the Policy. Concurrently, senior management should begin to develop integrated financial, human resource or operational performance reporting measures for PIAs so as to better understand the full costs associated with plans and priorities when seeking project funding.

In May 2002, the Treasury Board Secretariat committed to undertaking a comprehensive review of the provisions and operation of the PIA Policy within five years of its effective date. This review should also consider ways in which the PIA process and requirements therein can be streamlined to alleviate resource pressures within government.

Treasury Board Secretariat (TBS) Response:

TBS agrees with the Privacy Commissioner's recommendation and will explore options to streamline the PIA process and its requirements so that resources can be better managed and time pressures alleviated. In its current view, TBS has identified this as a priority issue that needs to be addressed in order to sustain the policy over the longer term.

PIA requirements need to be streamlined

1.95 In light of the significant resources required to conduct a PIA, and the shortages of such resources across government, there is a need to consider how best to ensure that some privacy analysis continues to be conducted while minimizing the draw on program and ATIP capacity. In addition to the PIA and PPIA protocols within institutions, it may be possible to create a third reporting structure (or privacy review) for smaller projects where full PIAs are not economically viable or timely. While such a process would not preclude or replace the use of PIAs, they may be used to streamline the administrative requirements of PIAs, balancing the need for some privacy analysis at program conception with other important operational considerations.

1.96 In other cases, as with shared service or system initiatives where entities use the same or similar approaches to the collection, use and disclosure of personal information, generic assessments might be better utilized. Enterprise resource planning and standardized records management systems would likely be ideal candidates for generic Privacy Impact Assessments.

1.97 We understand that the Treasury Board Secretariat is currently working on a Privacy Policy Suite Renewal Project which, among other things, will align Policy requirements with project risks. It is anticipated that the introduction of a privacy risk standard, to guide subsequent policy requirements and ultimate risk management strategies, will go a long way in streamlining the reporting requirements surrounding the current privacy impact assessment process.

Treasury Board Secretariat (TBS) Response:

TBS agrees with the Privacy Commissioner's recommendation and is committed to providing the necessary guidance and policy structure to enable institutions to better manage privacy risks. TBS is currently working to streamline the PIA policy requirements to enable institutions to address privacy risks in a manner that is commensurate to broader project risks. This will allow resources to be managed more effectively and institutions can focus on areas of particular risk.

More training capacity is needed

1.98 At an operational level, some institutions have developed good guidance and training to support their privacy impact assessment efforts. Combined with the Guidelines and e-learning tools provided by Treasury Board Secretariat, and the capacity to consult with the Office of the Privacy Commissioner, sufficient technical information is available to ensure that PIAs are complete and robust. Additional training and guidance is however needed to make program managers aware of their responsibilities under the Policy and to give them the privacy knowledge and skills necessary to conduct PIAs.

1.99 Since privacy impact assessment is a key federal component of the policy and program development process, we would expect the Treasury Board Secretariat, in conjunction with the Canada School of Public Service (the federal government's key training organization for senior managers) to reflect the policy in its suite of training courses. To date, only limited courses on the privacy impact assessment process are offered, and the School has not fully assessed how the Policy could impact its curriculum.

1.100 Recommendation: Given the obvious need for privacy training across government, the Treasury Board Secretariat, with assistance from the Canada School of Public Service, should assess how the Policy on Privacy Impact Assessments could be referenced in the courses it offers to senior managers in the federal public service. We believe that the Government should consider a strategic investment in privacy training and, at the very least, that current policy and program courses be referenced to the PIA Policy.

Treasury Board Secretariat (TBS) Response:

TBS will continue to pursue opportunities to build on its existing training and awareness initiatives, including senior management awareness, and will explore

options for privacy training through the Canada School of the Public Service. Training is an integral part of the privacy policy suite renewal process and the related implementation plan for the revised PIA policy components.

An absence of internal audit and evaluation

1.101 The PIA Policy states that the implementation of the Policy should be monitored, in part, through internal audits. Although some institutions have initiated or undergone internal privacy reviews over the past five years, including assessments of personal information holdings, none have conducted comprehensive audits for compliance with the PIA Policy, or of departmental PIA activities. While the ATIP divisions within select departments have recently begun to assume greater responsibilities in the oversight of PIA activities, the conduct of internal audits would complement and enhance institutional control activities and ensure that risks identified from the PIA process are sufficiently mitigated.

1.102 **Recommendation:** The Internal Audit Branches of all federal institutions subject to the Policy should seek to include privacy and PIA related reviews in their plans and priorities in the future, and to pursue the observations outlined in this report.

Treasury Board Secretariat (TBS) Response:

Where substantiated by risk analysis, institutions will be encouraged to conduct internal audits of their personal information handling practices and the related privacy management structure, including the PIA process.

Policy matters

Roles and responsibilities of OPC and TBS need to be reviewed

1.103 It is important to understand that the Privacy Commissioner of Canada is an independent Officer of Parliament and not an arm or extension of the government and the Treasury Board. The OPC has the discretion to review or not review any particular PIA and is not required to send comments to a department. We comment on PIAs when we see there is a need to do so. Similarly, approval by the OPC of a PIA (as should be sent to the OPC under the signature of the deputy head) is not required for a department to proceed with a project.

1.104 The intent of the PIA Policy is to ensure the Privacy Commissioner is informed and to demonstrate (to the satisfaction of the Privacy Commissioner) that risks to personal information have been identified and addressed. At the same time, in sending PIAs to the OPC, departments logically expect or desire feedback. They generally view any observations and recommendations from the OPC as "value added" and a means of ensuring that the PIA is well done. However, the risk is that the OPC is viewed as a de-facto quality control, which is not the intent of the Policy and inconsistent with the independence of the OPC. Whatever is done or not done regarding PIAs remains the sole responsibility and accountability of departments and agencies.

1.105 The current PIA Policy suggests that the OPC should be involved at the earliest reasonable stages of the development of a Privacy Impact Assessment. This intervention allows the OPC to analyze the steps taken to address potential privacy concerns, to ensure that the proper authority is in place to allow the

collection of Canadians' personal information, and to verify that the regulations and principles of the *Privacy Act* are being respected.

1.106 Although the completion of PIAs has always remained the responsibility of institutional heads, over the past several years we have witnessed an increased perception of *shared* responsibility for PIA quality and policy observance. In practice, as a function of the Commissioner's limited resources and given that PIAs are often submitted or reviewed close to program implementation, the OPC has effectively become a post implementation depository for PIAs rather than a consulting subject matter expert.

1.107 **The role of Privacy Commissioner should evolve.** In light of these developments, one must question whether or not the Privacy Commissioner should continue to play a role in the review of all Privacy Impact Assessments. Are there alternative enforcement instruments or reporting requirements which would better encourage compliance with the Policy? Could the OPC be more engaged upfront in the PIA process, through consultations, education and participation in training initiatives, thus better utilizing limited resources and better fulfilling its mandate as a privacy ombudsman?

1.108 The current practice allows the Privacy Commissioner to remain a prominent figure in perhaps the most central component of the federal government's privacy compliance regime. The requirement to submit all PIAs to the OPC for detailed review not only leads to a disclosure of institutional activities affecting privacy (an information gathering activity), but to the ability to enforce upon institutions privacy considerations in the development of those programs (if not compliance with the Policy outright).

1.109 While the PIA submissions review process most certainly contributes to improving the quality and completeness of institutional privacy analysis, one may argue that this review, in and of itself, is secondary in importance to the information and enforcement functions of the OPC noted above. As institutions become more skilled and adept at completing PIAs – and assuming significant investments in training and support – the contribution of OPC reviews towards quality and completeness may become less substantial going forward.

1.110 In examining alternative models that preserve the information and enforcement roles of the OPC in the PIA process, one might consider a system mandating institutions to submit only a summary notification of projects and PIAs, rather than a full PIA or PPIA for review. In practice, such disclosure already occurs in the most privacy sensitive of cases, where institutions contact the OPC to discuss planned initiatives and their potential privacy impacts prior to program development. These project notifications, if well designed and properly populated, could in turn serve as the basis for greater oversight and enforcement by allowing the Commissioner to request and review PIAs of interest, to follow-up on findings and recommendations, and to conduct entity specific or government-wide audits for compliance.

1.111 **The need for a federal privacy assessment registry.** In supporting a governance model whereby institutions are only required to submit summary notifications of projects involving personal information to the OPC, TBS may consider the need for a central database or registry of privacy impact assessments. Its purpose would be to provide a single window of access to PIAs and privacy intrusive projects across government, regardless of the responsible authority. The registry could be used by the public to better understand the substance and privacy impacts of government projects and by institutions such

as the Treasury Board Secretariat and the Privacy Commissioner to monitor PIA activities. The registry may also enhance the project management capability of institutions and work to reduce or eliminate PIA omissions.

1.112 The index concept, currently in use by federal institutions for strategic environmental assessment and Regulatory Impact Analysis Statements (for new regulations), may also improve the transparency of government operations and help to better engage the public and Parliamentarians on privacy matters.

Treasury Board Secretariat (TBS) Response:

TBS agrees with the Privacy Commissioner's recommendation and will work toward developing a centralized point of access to PIA related information. In the short term, TBS will focus its efforts on developing a comprehensive repository of PIAs as a means to enable a more comprehensive oversight of the policy and the administration of the *Privacy Act*. TBS will explore the development of an index over the longer term.

Improving oversight and enhancing reporting requirements

1.113 Enhancing the transparency of the privacy impact assessment process is critical to improving the quality of privacy analysis in government. Greater scrutiny generated by public exposure can prompt greater care in the preparation of PIAs and provide Parliament and the public with the necessary information to have more informed debates concerning privacy protection. Public disclosure may also provide additional assurance that privacy impacts are being appropriately considered in the development of programs, plans and policies – essentially holding each institution to account for the adequacy of the privacy analysis that was undertaken.

1.114 The *Privacy Act* currently requires federal institutions to account publicly for the collection, use and disclosure of personal information by ensuring accurate and up-to-date descriptions of Personal Information Banks in *Info Source*. In ensuring compliance with the Act and the PIA Policy, the Treasury Board Secretariat monitors disclosures made by institutions in *Info Source* as well as departmental Annual Reports to Parliament required by section 72 of the *Privacy Act*. As previously mentioned however, the reporting scorecard for institutions with respect to PIAs are quite minimal, and provide few measures to ensure that institutions are complying with the Policy. This is in contrast to the public reporting requirements of institutions under current Access to Information legislation.

1.115 **Recommendation:** To improve the quality of privacy analysis in the development of programs, plans and policies, and to better ensure compliance with the existing PIA Policy, the Treasury Board Secretariat should consider the need to enhance and expand the reporting requirements for privacy impact assessments in departmental annual reports. Revised reporting requirements should include, at a minimum, a disclosure of:

- The number and nature of projects involving the use of personal information initiated during the year;
- The nature of program changes or re-designs with potential privacy impacts;
- The status of PIAs for each project identified above;

- References to completed PIA summaries where Privacy Impact Assessments have been completed; and
- Cases where programs, services, plans or policies were implemented during the year in the absence of privacy impact assessment, if any.

The Treasury Board Secretariat, as the central authority responsible for monitoring compliance with the PIA Policy, should also consider the above mentioned reporting requirements in strengthening its oversight capacity.

Treasury Board Secretariat (TBS) Response:

TBS agrees with the Privacy Commissioner's recommendation and will explore options for revising the reporting requirements related to PIAs to those elements identified by the OPC. TBS is also committed to improving the oversight mechanisms as part of its policy suite renewal exercise. This means strengthening existing reporting mechanisms to ensure that relevant information is made available to the OPC and to TBS, to enable each organization to fulfill their respective legislative responsibilities for oversight and monitoring.

The need for strategic privacy impact assessment

1.116 The existing TBS policy for PIAs was designed to assess the privacy impacts of government initiatives on a program by program basis, at the time at which they are conceived. There is a need however to deal with the broader privacy implications of plans and policies that may not be easily addressed at the project or service level. What may be termed "strategic privacy impact assessment", a non-legislated process for the privacy assessment of federal policy and plans submitted to Cabinet consideration, may be one such tool for dealing with these initiatives.

1.117 Over the past several years, the Government of Canada has embarked on (or initiated discussions for) several programs with potentially serious effects on the public's privacy, for example: the Government On-line project, the Smart Border Accord, the creation of a "no-fly" list and the establishment of Services Canada, to name but a few. Due to the sheer magnitude and pervasive nature of such initiatives, the implementation of these government plans and others (e.g., surveillance) will require comprehensive privacy consideration and analysis.

1.118 Although the Office of the Privacy Commissioner, through appearances before Parliamentary committees and bilateral discussions with government institutions, attempts to comment on such plans early in the legislative process, it is often too late when a bill has been introduced into the House of Commons to rethink approaches to information issues. According to the Commissioner, the public interest would be better served by engaging the OPC earlier on in the process and by providing institutions with more time to respond to privacy concerns.

1.119 Knowing the potential privacy impacts of proposed policies and plans would provide Cabinet with an early opportunity to adjust or modify programs to protect the personal information of Canadians, and to reduce future costs associated with program changes. In the absence of some strategic privacy impact assessment tool, we believe the government's privacy policy suite will risk falling short of meeting its promise in guiding policy, plan and program development.

1.120 Recommendations: The Privy Council Office, as the central authority responsible for managing Cabinet's decision-making system, should consider the need for strategic privacy impact assessment and how best to integrate privacy considerations into proposals prepared for Ministers and for Cabinet consideration.

Privy Council Office (PCO) Response:

The federal government is committed to both the protection of privacy in its own operations and to the general principles of fair information practices. The PCO supports the Privacy Impact Assessment (PIA) process under which the Deputy Ministers and other deputy heads of institutions are responsible for determining whether initiatives have a potential impact on the privacy of Canadians and for integrating and balancing privacy with other legislative and policy requirements.

Certainly identification of privacy issues at the earliest stage of project planning is ideal. We agree that this information could provide Cabinet and deputy heads with the opportunity to modify a planned initiative to perhaps better protect personal information and eliminate additional costs to program development.

PCO commits to working with Treasury Board Secretariat, who is responsible for the PIA process, on its Privacy Policy Suite Renewal Project, to ensure that the necessary privacy analyses are undertaken into proposals for Ministers and for Cabinet consideration. This consultation will also consider how to assess not just the impact of individual programs, but also how to be more strategic by considering if there are any recommended in the Commissioner's report.

Assessing the cumulative effects of plans and policies

1.121 Concerns are often raised about the long-term changes that may occur to an individual's privacy, not only as a result of a single isolated action but by the combined effects of each successive and interdependent intervention. Indeed, the incremental effects on the integrity of personal information may be significant from a privacy point of view even when the effects of each successive action, independently assessed, are considered insignificant.

1.122 To ensure the incremental effects resulting from the combined influences of various actions are properly assessed, PIAs should consider the cumulative privacy effects that are likely to result from a program in combination with other projects or activities that have or will be carried out. Currently, the PIA Policy does not explicitly require such an analysis in individual PIA submissions.

1.123 Although the assessment of cumulative privacy impacts presents some inherent difficulties (given the complexity of issues and the challenges in obtaining complete information), the committee structures already employed by many institutions to review PIAs presents an ideal setting in which to begin engaging in cross-departmental consultations. The assessment of cumulative effects is already seen as representing best practice in conducting environmental assessments, and is now required in federal legislation when an action is subject to review under the *Canadian Environmental Assessment Act*.

1.124 Recommendation: As part of its Privacy Policy Suite Renewal Project, the Treasury Board Secretariat should work with federal institutions to encourage the assessment of cumulative privacy effects in PIAs, where

appropriate, and to develop practical guidelines to assist in such analysis. Similar consideration should be given to entities with multiple departmental portfolios (such as Public Safety and Emergency Preparedness) as a means of coordinating and fully responding to privacy risks associated with large scale programs.

Treasury Board Secretariat (TBS) Response:

TBS agrees with the Privacy Commissioner's recommendation and will examine ways to asses the cumulative privacy effects of large-scale programs or initiatives, including those at entities with multiple government institutions, as part of the PIA process.

Conclusion

1.125 It has been five years since the Policy on Privacy Impact Assessments was introduced. The overall results of our audit suggest that some institutions have made serious efforts to apply the directive, but that still more effort is required to ensure that the Policy is having its desired effect. There are important gaps in the Policy's application, and many institutions are just beginning to implement the management frameworks required to support the PIA process.

1.126 Although the Policy was designed to ensure that privacy protection is a key consideration in the initial framing of a project's objectives and activities, privacy analysis is not always completed at the time of program conception. In some instances, PIAs are not completed at all. The PIA process in most institutions is far from being fully integrated into the overall risk management strategies of individual entities and, in such cases, fails to influence the development of new programs, plans and policies.

1.127 The primary reasons for the uneven application of the Policy and for the performance failures identified are: a lack of management support and infrastructure, the limited integration of PIAs into the strategic decision making process, shortages in privacy resources, a lack of training capacity, and the absence of internal evaluation and oversight.

1.128 As the Treasury Board Secretariat undertakes a review of the Policy, it should consider the need to streamline the PIA process for projects of low risk, and the need to mandate the assessment of the cumulative effects of programs and services within the PIA process. The TBS should also review the role of the Office of the Privacy Commissioner in the PIA process, and seek to strengthen the PIA and privacy reporting requirements of federal institutions. Finally, the TBS should consider how best to reinforce the link between the PIA Policy and relevant legislation and evaluate any corresponding resource impacts.

1.129 In addition to the PIA requirements for new (or substantially redesigned) programs and services, the Privy Council Office should consider introducing a process for evaluating the potential privacy impacts of proposed policies and plans before Cabinet. Strategic privacy impact assessment would provide government with the opportunity to more fully assess the pervasive privacy effects of new plans and priorities prior to their introduction at the departmental or program level.

About the Audit

Objectives

1. To determine if federal institutions are conducting privacy impact assessments effectively and in compliance with the Policy.

   Sub-objectives:

   a. To measure the extent to which entities government-wide have effective management control frameworks or administrative infrastructures in place to support the conduct of PIAs (including the ability to identify those instances where a PIA is required).

   b. To establish whether individual institutions have formally identified all activities requiring a privacy impact assessment, and whether these activities have been sufficiently researched and documented in complying with the PIA Policy and Guidelines.

   c. To establish whether performance monitoring is effectively conducted on key financial, operational and human resource aspects of PIA operations in each institution.

2. To determine whether the Policy has been successful in achieving its original objectives (given the larger accountabilities or requirements under the *Privacy Act* or related privacy policies), and to examine the role of central institutions in managing the PIA process government-wide.

Scope and approach

Although the Policy applies to all departments and agencies subject to the *Privacy Act*, the audit focused on nine departments and agencies active in the collection, use and dissemination of personal information. In selecting such departments, we considered specific parameters such as the volume and sensitivity of personal information handled, evidence of significant system or program investments, and the results of past reviews, including evidence of possible non-compliance with the Policy based on the Office's own assessment of PIA/PPIAs submitted for review over the last two years.

In addition to the detailed audit work conducted on these nine entities, we conducted a survey of 47 additional institutions subject to the Policy and *Privacy Act*, asking each to self-assess against the same four evaluation criteria used in our primary review. We believe that the survey results, in combination with our detailed audit findings, provide the report with additional breadth and depth, and make for a better overall assessment of the federal government's application of the Policy.

The departments and agencies we audited, along with the corresponding audit objectives they were assessed against are identified in Table 1. Each of the audit objectives is accompanied by a series of criteria against which performance was evaluated (see Table 2).

Some quantitative information in this report is based on data drawn from various federal and other sources. We are satisfied with the reasonableness of the data in the context of this report, however, the data has not been audited, unless otherwise indicated.

Audit team

Assistant Commissioner: Raymond D'Aoust
Director General: Trevor Shaw

Lead Auditor and Report Author: Navroze Austin

Bill Wilson, Breckenhill
Ned Eustace, Breckenhill

Table 1 • Departmental and agency coverage by audit objectives

Federal institution	Audit objectives			
	1 a	1 b	1 c	2
Canada Revenue Agency	■	■	■	■
Citizenship and Immigration Canada	■	■	■	■
Correctional Service Canada	■	■	■	■
Health Canada	■	■	■	■
Human Resources and Social Development Canada	■	■	■	■
Indian and Northern Affairs Canada	■	■	■	■
Royal Canadian Mounted Police	■	■	■	■
Services Canada	■	■	■	■
Veterans' Affairs Canada	■	■	■	■
Central organizations				
Treasury Board Secretariat	□	□	□	■
Privy Council Office	□	□	□	■
Office of the Privacy Commissioner	□	□	□	■

■ Assessed against objective □ Not assessed against objective

Entities surveyed (self-assessed)

Agriculture and Agri-Food Canada
Atlantic Canada Opportunities Agency
Business Development Bank of Canada
Canada Border Services Agency
Canada Firearms Centre
Canada Mortgage and Housing Corporation
Canada Post Corporation
Canada School of Public Service
Canada Science and Technology Museum
Canadian Air Transport Security Authority
Canadian Centre for Occupational Health and Safety
Canadian Food Inspection Agency
Canadian Forces Grievance Board
Canadian Human Rights Commission
Canadian Human Rights Tribunal
Canadian Institutes of Health Research
Canadian International Development Agency
Canadian Museum of Civilization Corporation
Canadian Museum of Nature
Canadian Radio-television and Telecommunications Commission
Canadian Security Intelligence Service
Canadian Wheat Board
Commission for Public Complaints Against the Royal Canadian Mounted Police
Copyright Board Canada
Department of Justice Canada
Elections Canada
Environment Canada
Export Development Canada
Farm Credit Canada
Fisheries and Oceans Canada
Foreign Affairs and International Trade
Immigration and Refugee Board
Indian Residential Schools Resolution Canada
Industry Canada
Library and Archives Canada
National Arts Centre
National Defence
National Parole Board
Office of the Registrar of Lobbyists
Pensions Appeal Board
Privy Council Office
Public Safety and Emergency Preparedness Canada
Public Service Commission of Canada
Public Service Labour Relations Board
Public Works and Government Services Canada
Statistics Canada
Transport Canada

Table 2 • Audit criteria

Audit objective	Criteria
1 a	▪ Objectives and goals of the PIA process are clearly defined, formally approved and effectively communicated. ▪ Specific PIA-related accountabilities are established within the institution. ▪ The organizational structure for the PIA process is formally and effectively supported. ▪ PIA-related policies, regulations and guidelines are identified, evaluated and incorporated into operational activities. ▪ Control activities and mechanisms for the PIA process are in place, relevant, comprehensive and address known risks. ▪ An effective oversight function for the PIA process is in use.
1 b	▪ PIAs are conducted for proposals for all new programs and services, and for substantially redesigned programs and services, which raise privacy risk. ▪ Responsibility for the PIA process is formally assigned within the affected program/service area. ▪ Initiation and definition of the scope of PIAs are completed in the early stages of the design or re-design of a program or service. ▪ The institutional official responsible for PIAs ensures that accountable Program and Service officers are made aware of the need to have the OPC review PIAs, once approved by the Deputy Head. ▪ Final PIA summaries are readily accessible within the institution and to the public and are made available to the public in a timely manner. ▪ Risk evaluation, implications and possible mitigation or resolution recommendations are identified and documented as part of the PIA process. ▪ Privacy analysis adheres to, and documents, the privacy principles and applicable legislation and policies. ▪ PIAs are maintained so that privacy risks are identified and then resolved, mitigated or identified as unresolved. ▪ PIA reports either provide assurance that the privacy risks associated with program and service delivery activities have been mitigated to the greatest extent possible or, conversely, serve as early warning that significant privacy risks require resolution. ▪ PIA risk mitigation action plans are formally tracked and results are reported to management.
1 c	▪ Operational performance expectations and results for PIAs are reported to management. ▪ Financial performance expectations and results for PIAs are reported to management. ▪ Integrated financial and operational performance reporting for PIAs is developed and reported to management. ▪ Both human resource performance expectations and their results regarding PIAs are developed and reported to management.
2	General considerations: ▪ Have the Policy and supporting Guidelines been effective in achieving the desired results? ▪ What conclusions, if any, can we draw from the results of the PIA review as to privacy management practices government wide? ▪ How does the PIA process in Canada compare to that of other jurisdictions (provincial and international)? ▪ Is there a management framework in place at the government centre and is it appropriately designed and implemented to provide Policy oversight? ▪ What role should Parliamentarians play in advancing privacy matters and supporting the PIA Policy? ▪ Other matters.