Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Privacy Impact Assessment Audit Guide

Canada

Privacy Impact Assessment

Audit Guide

Table of Contents

Acronyms, Abbreviations and Definitions in this Guide

Acronyms and Abbreviations

ATI.....Access to Information
ATIP.....Access to Information and Privacy
BPD.....Business Process Diagram
EPA.....Effective Project Approval
GSP.....*Government of Canada Security Policy*
MGI.....*Management of Government Information Policy*
MGIH.....*Management of Government Information Holdings Policy*
MOU.....Memorandum of Understanding
OPC.....Office of the Privacy Commissioner
PPA.....Preliminary Project Approval
PIA.....Privacy Impact Assessment
PPIA.....Preliminary Privacy Impact Assessment
TBS.....Treasury Board of Canada Secretariat
TRA.....Threat and Risk Assessment

Definition

PIA Coordinator: The term PIA Coordinator is used throughout this Audit Guide in reference to a person, position or group that is responsible for and coordinates the PIA process in a federal institution. It is recognized that the PIA function will be organized and managed differently across federal government institutions. For example, responsibility for the PIA function may rest with an ATIP officer, a Program Manager, a full-time PIA Practitioner, a part-time PIA Team, or an employee who has PIA coordination among other responsibilities. In keeping with the intent of the *PIA Policy*, this Guide is not intended to influence how a PIA coordinator position should be resourced or organized.

PIA Glossary of Terms: http://www.cio-dpi.gc.ca/pgol-pged/piatp-pfefvp/assistant/glossary/glossary_e.asp

Preface

This Audit Guide has been prepared to assist federal institutions in auditing the implementation of the *Privacy Impact Assessment* (PIA) *Policy*. The *PIA Policy*, introduced by the Government of Canada on May 2, 2002, requires institutions to consider the impact of new programs and services on the privacy rights of Canadians.

The Audit Guide can be used in three ways:

- First, it presents the policy requirements, along with related information and key sources for understanding the basics of the PIA process;
- Second, it provides background information to broaden the reader's understanding of the responsibilities of key stakeholders involved in completing, reviewing and approving PIAs; and
- Third, it proposes audit objectives and criteria so that Internal Auditors may develop a customized audit program using a risk-based audit approach.

The Treasury Board of Canada Secretariat (TBS), with support from the TBS Centre of Excellence for Internal Audit and an interdepartmental committee of federal government Internal Auditors and privacy practitioners, has prepared this Audit Guide to promote a common understanding of the application and audit of the *PIA Policy* in the federal government.

Section 1. Audit Guide Use and Organization

Guide Use

This Guide is intended as a reference tool for Internal Auditors in the Government of Canada and may also be of assistance to the privacy community, including PIA Coordinators. It was developed under the guidance of the Interdepartmental PIA Audit Guide Advisory Committee as well as representatives from the Office of the Privacy Commissioner (OPC) and the TBS Centre of Excellence for Internal Audit.

The Guide has been structured to prepare Internal Auditors for the broad range of review activities that are inherent in the PIA process. Given that many institutions are in the early stages of implementing the *PIA Policy*, Internal Auditors will be able to adjust to their respective environments by tailoring their engagements based, in part, on the suggested audit objectives, criteria and audit steps presented in this Guide. Internal Auditors will need to apply a risk-based approach to assist them in identifying areas of highest risk and in developing audit objectives and criteria to address these risks.

In this Guide, information is first given on the *PIA Policy* and its intent, that is, why the Government of Canada established the *PIA Policy*, what a PIA process looks like and how a PIA is conducted in government institutions. The Guide then provides audit objectives and criteria that deal with the soundness of the related management framework, compliance with the *Policy*, and performance measurement. Background information is given to supplement research.

Audit objectives and criteria serve as suggestions for planning, scoping and preparing a PIA audit program. For ease of reference, policy-compliant audit criteria are shaded throughout the checklists. Also, based on discussions with the Interdepartmental PIA Audit Guide Advisory Committee, some members noted that they might first test the audit objectives and criteria through a pilot review of a specific PIA Report, rather than starting with an assessment of the related management control framework or performance of an institution. As a result, Checklist 7 lists only policy-compliant criteria, under an objective to determine if a particular PIA is in compliance with the *PIA Policy*.

Guide Organization

The Audit Guide is organized into three parts:

Sections 1-6: The requirements of the *PIA Policy* and context for the Audit Guide are provided in the body of the Guide.

Section 7: PIA audit objectives and criteria are provided in Section 7, entitled Audit Elements. The objectives and criteria, along with possible audit steps, are presented at the end of this Guide in a checklist or 'working version' format.

Appendices: Appendices cover PIA related accountabilities, examples of practices used in selected federal institutions, additional PIA audit references with Internet websites/links and a working version of the PIA audit objectives and criteria.

Section 2. Scope of the Audit Guide

The Audit Guide is intended for use in all federal institutions subject to the *Privacy Impact Assessment Policy*. The *Policy* applies to some 150 departments, agencies and Crown corporations. A list of these institutions, with the exception of the Bank of Canada, can be found in the Schedule to the *Privacy Act* (see http://laws.justice.gc.ca/en/P-21/93727.html#rid-93753).

The scope of this Guide is limited to the responsibilities of institutions in implementing the *PIA Policy*. The Guide does not address the larger accountabilities or requirements under the *Privacy Act* or related policies. Audit guidance is restricted to verifying whether or not PIA processes have enabled a given institution to comply with the *PIA Policy* in an effective manner.

It is recommended that Internal Auditors refer to the *PIA Policy*, *PIA Guidelines* and the PIA e-learning tool, first, in order to learn more about how departments and agencies might organize their business practices to be in compliance with the *PIA Policy*.

The *PIA Policy*: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp

The *PIA Guidelines*: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp

The PIA e-learning tool: http://www.cio-dpi.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp

Section 3. Assumptions

In conducting an audit of the implementation of the *PIA Policy*, it is assumed that the Internal Auditor possesses the knowledge, skills and other competencies needed to perform the engagement and to understand the risk-based audit methodology indicated in this Guide. Should the Internal Auditor or audit team not possess these competencies, it is assumed that such competencies would be acquired to support the audit engagement.

It is further assumed that PIA audits will be completed in accordance with professional internal auditing standards.

Section 4. Overview of the PIA and Preliminary PIA Processes

4.1 What is a PIA?

A PIA refers to a comprehensive process for determining the effects of program and service delivery initiatives on individual privacy. The PIA process is a useful methodology to ensure that privacy is built in at the outset of any new program or service and to assure the public that their privacy is safeguarded.

4.2 When is a PIA required?

Departments and agencies:

- Must conduct PIAs for proposals for all new programs and services that raise privacy risks;
- Must undertake PIAs if they are substantially re-designing programs or services or their delivery channels, or transforming them for electronic service delivery in a manner that affects the collection, use or disclosure of personal information; and
- May consider developing PIAs for existing programs and services, for which no changes are proposed, if no previous privacy assessments exist or if there are outstanding privacy risks.

4.3 When is a Preliminary PIA (PPIA) required?

Early in the design phase of a program or service, PPIAs may be conducted when an institution doesn't have enough detailed information required for a comprehensive assessment or scoping of privacy-related risks, or to determine whether there are privacy-related risks that warrant a PIA.

PPIAs identify the types and volumes of personal information to be collected, used and disclosed. They verify legislative and policy authorities for the proposed program or service. They also clarify the roles, responsibilities and legal and policy status of the key stakeholders, including other jurisdictions and the private sector.

The *PIA Policy* notes that PPIAs involve a determination of the aspects of the new program and service that are likely to involve privacy risks along with potential risk mitigating options. Early consultation with the OPC is strongly recommended at the early stages of the initiation of a project to determine whether or not there is a need for a full PIA.

4.4 What are the main steps for completing a PIA?

The *PIA Policy* provides the following four-step approach for completing a PIA:

Step 1 – Project Initiation: Once it is determined that personal information is being collected, used or disclosed in a proposed initiative, the scope of the initiative should be defined, the required resources for the project should be determined and PIA tools should be adapted to reflect the nature of the project/proposal and the scope of the PIA. At this stage, it may be decided that a PPIA should be conducted, which will enable the institution to determine whether a full PIA is required. Typically, this step assembles necessary documentation and all relevant legislation that has implications for privacy or personal information protection. This step is also used to identify key stakeholders whose involvement will assist in the completion of the privacy analysis. At a minimum, identification of the legal authority and justification for the project/proposal should be documented.

Step 2 – Data Analysis: Data analysis includes graphical representations of the business processes involved, determination of logical clusters of personal information and detailed data flow charts.

Step 3 – Privacy Analysis: Privacy analysis is assessed through completion of one of two questionnaires that identifies the specific privacy risks and provides an analysis of the options to resolve or mitigate these risks.

Step 4 – PIA Report Completion: The PIA Report evaluates privacy risks, and determines risk mitigation options and recommends actions to mitigate risks. The PIA Report, "constitutes a policy-level discussion of the program or service" in order to facilitate policy and informed system design decisions.

Guidance from the *PIA Policy* states that a multi-disciplinary team of officials at the institutional level is needed to complete a PIA. These include legal experts, access to information and privacy experts, program and systems managers and security and technical experts.

4.5 What might an overview of a typical PIA process look like?

The following potential scenario is used in the PIA e-learning tool to describe the process of initiating, managing and approving a PIA:

1. The process begins with a project head/program or service manager asking the question: Is personal information being collected, used or disclosed in this initiative?
2. Privacy experts at the institution (usually the Privacy Coordinator or Access to Information and Privacy [ATIP] personnel) may be consulted if the answer to the above question 1 is 'yes'.
3. Once privacy experts are involved and advice is received, a decision on the need for a PIA or PPIA is made.
4. If a project head/program or service manager has been assigned to complete a PIA, the manager may create a PIA Team, appoint a PIA Practitioner, or a reporting structure where responsibilities for the project are defined.
5. A PIA is then completed collaboratively with the PIA Team (e.g. legal and privacy experts, ATIP Office, Systems Analysts and any required Departmental Committees).
6. During the conduct of a PIA the Office of the Privacy Commissioner (OPC) may be consulted, following institutional procedures.
7. Once a PIA has been completed, there may be an internal review process that can involve a Director, a Director General, and an Assistant Deputy Minister. At any point in the review process, the PIA may require revisions.
8. Once the review process is complete, the Deputy Head will review the PIA and may request revisions. If necessary, the PIA is then sent back to the PIA Team, PIA Practitioner or PIA Manager.
9. Once the Deputy Head reviews and provides approval on the PIA, the *PIA Policy* requires that it be sent to the OPC for review.

10. The OPC reviews the PIA and provides advice and recommendations for the institution to consider.
11. Institutions decide on appropriate actions and the Deputy Head provides a final sign-off on the PIA. Institutions respond to the OPC comments.
12. Institutions make summaries of the results of their PIAs available to the public in a timely manner (usually on the institution's Website), using plain language.

4.6 The PIA e-learning tool

To support federal institutions in understanding the goals of the *PIA Policy* and in developing PIAs, the TBS has developed *PIA Guidelines* and a PIA e-learning tool. The PIA e-learning tool provides assistance on how to prepare a PIA, addresses potential privacy risks, and identifies courses of action for consideration when developing risk-mitigating strategies. Users of the PIA e-learning tool are able to:

- Complete an education module where they learn how different legislation and policies promote privacy protection in Canada.
- Understand how to "manage" the development of a PIA.
- Be tutored as they complete an assessment of PIA activity and prepare a PIA report through an interactive "PIA Assistant".

The PIA e-learning tool is at: http://www.cio-dpi.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp

It is worthwhile for Internal Auditors to review the PIA e-learning tool. Following a quick review of the tool, Internal Auditors will understand the importance of involving key stakeholders in the PIA process and can consider the best-fit approach to structuring risk analysis.

Section 5. Closely Related References

The following federal government legislation, policies and audit guides are pertinent. It is recommended that these references be reviewed and understood prior to the development of an audit program to assess the implementation of the *PIA Policy*:

- *Guide to the Audit of Security* DRAFT (2003) lists safeguards essential for limiting access to personal information. It details information technology designs and features that lead to appropriate protection of personal information. The Guide details when and why Threat and Risk Assessments (TRA) are required in the assessments of networks and databases. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TB_H4/gas_e.asp

- *Guide to the Review of Management of Government Information Holdings* (*MGIH*) (1995) – even though this Guide is based on the outdated *MGIH* Policy, it can be used to review the management of the information lifecycle. The Guide lists good practices in the establishment of limited collection processes.
  http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/GUIDE_e.asp
- *Management of Government Information Policy* (2003*)* addresses the management of government information by federal institutions. It identifies that 'federal government institutions must manage information in a privacy protective manner'. The Policy reiterates requirements for limiting the collection, use and disclosure of personal information to a minimum.
  http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp
- *Privacy Act* and *Regulations* (1983; R.S. 1985) govern collection, use, disclosure and retention of personal information by federal government institutions listed in the Schedule to the *Privacy Act*.
  http://laws.justice.gc.ca/en/P-21/index.html
- *Privacy and Data Protection Policy* (1993) provides guidance on interpreting the *Privacy Act* and on the collection, use, disclosure and retention of personal information by federal institutions. A number of sub-policies are found with specific directions on data matching, use of the Social Insurance Number, roles and responsibilities for privacy in an institution and collection of personal information.
  http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-1_e.asp
- *Project Approval Policy* (revised 2001) ensures that selected projects proposed for approval by the Treasury Board be supported by documentation that adequately describes the full scope of the project including the associated management framework. Normally, the first submission by a department seeks Preliminary Project Approval (PPA) and authority to proceed with all or part of the project's definition phase. When the project is fully defined, the department submits for Effective Project Approval (EPA) to obtain authority to implement the project. EPA may be contingent on the successful completion of a PIA.
  http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_122/chap2-1_e.asp
- The Enhanced Management Framework for Information Management and Information Technology provides an overall structure for the management of information technology projects, and may be useful to the Internal Auditor in understanding the basic project management environment for systems development that must deal with privacy risk.
  http://www.cio-dpi.gc.ca/emf-cag/index_e.asp

(**Note**: See APPENDIX C for the list of ancillary policies and reference sources that may be of assistance when conducting a PIA audit.)

Section 6. PIA Management Issues

In the conduct of a PIA audit, the Internal Auditor may be asked to answer a number of risk related questions based on management practices and issues identified during the engagement, such as: how well has the institution adjusted to the requirements of the *PIA Policy*, or how well has the institution been able to meet the objectives of the *Policy* through its practices or processes?

Other questions that may be asked regarding the *PIA Policy* include the following:

- Has awareness of the *PIA Policy* been raised sufficiently in the institution?
- Is there an official or group responsible for identifying and informing program or service initiators that they must complete a PIA?
- Are there instances where the institution's projects that involved the collection, use and disclosure of personal information warranted the conduct of a PIA, but were initiated without the benefit of a PIA or a PPIA?
- Has the institution misunderstood its obligations within the *PIA Policy* (e.g. has the PIA process been defined only through a simple template checking exercise)?

Questions on management issues related to the *PIA Policy* may include:

- In preparing PIAs, are the *PIA Policy Guidelines* followed?
- Does it appear that the institution is obtaining and retaining the expertise required in the areas of privacy analysis, risk analysis, and Threat and Risk Assessments (TRAs)?
- What is the general level of effort/investment required from key stakeholders (i.e. appropriate officials from program, security, legal, privacy and information technology areas) to complete a PIA?
- Are the costs of conducting PIAs identified and integrated into the design of a program or service, or are they recorded as 'corporate overhead'?

Section 7. Audit Elements

Overall Objective

To determine if federal institutions have implemented the *Privacy Impact Assessment (PIA) Policy* with due regard to effectiveness and are conducting PIAs in compliance with the Policy.

Organization

The first six audit objectives present the foundation for developing an audit program. These objectives address the management control framework for PIAs, compliance to *PIA Policy*, and related performance measurement. The seventh objective repeats the compliance criteria that can be used to audit the conduct of a single PIA.

The compliance-related audit objectives are centered in objectives 2 through 5. These objectives reflect the main responsibilities of institutions, namely:

- To conduct PIAs for all new programs and services (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 implementation of the initiative, program or service;
- To develop a risk assessment and mitigating measures for privacy risks identified; and
- To make PIA summaries public.

For easy identification, all mandatory or compliance criteria are shaded below and in the Audit Checklists at the end of this Guide.

Management Control Framework

Objective 1: To identify whether an effective management control framework is in place to support the conduct of PIAs.

We would expect to find:

1.1 Objectives and goals of the PIA process are clearly defined, formally approved and effectively communicated.

1.2 Specific PIA-related accountabilities are established within the institution. (*PIA Policy*, Accountability Sections 1-3)

1.3 The organizational structure for the PIA process is formally and effectively supported.

1.4 PIA-related policies, regulations and guidelines are identified, evaluated and incorporated into operational activities.

1.5 Control activities and mechanisms for the PIA process are in place, relevant, comprehensive and address known risks.

1.6 An effective oversight function for the PIA process is in use.

Conducting PIAs

Objective 2: To establish whether the institution has formally identified all activities requiring a PIA process and has researched and documented these activities in compliance with *PIA Policy* and *Guidelines*.

Objective 2.1: To determine if the scope of work required to identify and process a PIA or a PPIA is properly defined.

We would expect to find:

2.1.1 PIAs are conducted for proposals for all new programs and services, and for substantially redesigned programs and services, which raise privacy risk. (*PIA Policy*, Section 2)

2.1.2 New programs and services, and substantially redesigned programs and services, are defined through a formal Business Case.

2.1.3 Programs and services identified in PIAs refer to the legislated authority, regulation and policies applicable to the collection, use and disclosure of personal information. (*PIA Policy*, Section 1)

2.1.4 Responsibility for the PIA process is formally assigned within the affected program/service area.

2.1.5 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. (*PIA Policy*, Section 2)

Objective 2.2: To determine whether business processes subject to a PIA or PPIA are documented sufficiently to support the requirements of the PIA process.

We would expect to find:

2.2.1 Guidelines are available directing Programs and Services, subject to a PIA, on how to document business processes.

2.2.2 Responsibility for the management of business processes and the flow of personal information is identified and documented.

2.2.3 Institutions identify all personal information found within business processes. (*PIA Policy*, Section 3)

2.2.4 The relationship between personal information and other types of information (e.g. business confidential information) is assessed.

2.2.5 Outcomes from relevant TRAs, or TRA updates, are identified and appropriately applied.

2.2.6 PIA reports include the minimum required information. (*PIA Policy*, Section 5)

Notification to the Office of the Privacy Commissioner

Objective 3: To determine whether the institution's notification to the OPC complies with the *PIA Policy*.

We would expect to find:

3.1	Institutional practices require that final PIAs are formally approved by the institution's Deputy Head, and sent to the OPC prior to implementation of new activities. (*PIA Policy*, Section 7)
3.2	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.
3.3	Documents supporting the completion of PIAs are made available to the OPC.
3.4	All formal OPC responses to institutional requests for PIA information, as well as institutional replies to the OPC, are formally retained by the institution.

Publication of PIA Summaries

Objective 4: To establish whether institutions publish final PIA summaries in compliance with the *PIA Policy*.

We would expect to find:

4.1	Final PIA summaries are clearly written in both official languages. (*PIA Policy*, Section 7)
4.2	PIA summaries undergo ATIP review prior to publication.
4.3	Draft PIA summaries are forwarded for review to the responsible communications function prior to publication.
4.4	Final PIA summaries are readily accessible within the institution and to the public.
4.5	Final PIA summaries are made available to the public in a timely manner. (*PIA Policy*, Section 7)

PIA Risk Mitigation Measures

Objective 5: To determine whether risks identified from the PIA process are sufficiently mitigated.

We would expect to find:

5.1	Risk evaluation, implications and possible mitigation or resolution recommendations are identified and documented as part of the PIA process. (*PIA Policy*, Section 5)

5.2 Functional specialists addressing PIA risks identify early awareness and knowledge of common risks associated with changes to program or service delivery.

5.3 Business processes and data flow tables are documented in support of risk identification and assessment.

5.4 Risks identified at the branch, function or institutional levels are escalated, as appropriate.

5.5 Privacy analysis adheres to, and documents, the privacy principles and applicable legislation and policies. (*PIA Policy,* Section 4)

5.6 PIAs are maintained so that privacy risks are identified and then resolved, mitigated or identified as unresolved. (*PIA Policy,* Section 1)

5.7 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 Policy,* Section 6)

5.8 PIA risk mitigation action plans are formally tracked and results are reported to management.

Comprehensive Performance Assessment

Objective 6: To establish whether performance monitoring is effectively conducted on key financial, operational and human resource aspects of PIA operations in the institution.

We would expect to find:

6.1 Operational performance expectations and results for PIAs are reported to management.

6.2 Financial performance expectations and results for PIAs are reported to management.

6.3 Integrated financial and operational performance reporting for PIAs is developed and reported to management.

6.4 Both human resource performance expectations and their results regarding PIAs are developed and reported to management.

APPENDIX A – PIA Accountabilities

Stakeholders	Accountabilities
Heads of Institutions	▸ Ensures institutions comply with the Privacy Act, Regulations and associated policies, including the *PIA Policy*.
Deputy Heads of Institutions	▸ Determines whether or not changes to programs and services have a potential impact on privacy and, therefore, warrant the development of a PIA. ▸ Establishes processes for consulting with the Office of the Privacy Commissioner. ▸ Approves the PIA prior to its submission to the OPC. ▸ Determines how to respond to any advice from the OPC. ▸ Approves the final PIA. ▸ Promotes awareness of *PIA Policy* requirements. ▸ Ensures that the process and tools used in a PIA are rigorous. ▸ Ensures that summaries of results of PIAs are available to the public.
Treasury Board of Canada Secretariat	▸ Maintains, reviews, advises and supports *PIA Policy* and *PIA Guidelines*. ▸ Monitors compliance through a variety of mechanisms such as: – Project approval and funding—Institutions seeking Preliminary Project Approval from TBS pursuant to the *Project Approval Policy*, must include the results of a PIA in their submissions or the project brief. Institutions seeking Effective Project Approval from TBS must provide a status report in their submissions or the project, briefly summarizing the actions taken or to be taken to mitigate privacy risks. – Institution's Annual Reports to Parliament - Privacy Act (Section 72) – Departmental audits and review reports.
Privacy Commissioner	▸ Provides advice to institutions as they conduct PPIAs or PIAs. ▸ Reviews final PIAs.
Institutions	▸ Determines the need for conducting PIAs. ▸ Develops and maintains PIAs to evaluate whether a program or service delivery initiatives complies with privacy requirements. ▸ Resolves or mitigates privacy risks identified in the PIA process. ▸ Ensures that PIAs are a shared management responsibility that includes the co-operation and support of various officials throughout the institution including program and project managers, privacy policy advisors, legal experts, functional specialists and communications experts.

APPENDIX B – Two PIA Delivery Models

To better understand how institutions have implemented the *PIA Policy*, the Interdepartmental Privacy Impact Assessment Audit Guide Advisory Committee invited departments to describe the processes they use to administer the *PIA Policy*. Two examples of PIA delivery models, for a large and a mid-sized institution, are presented as follows:

For one large institution:

A committee is established to assume an oversight role. An official will be designated, or a working committee assigned, to develop an institutional *PIA Policy*.

Regarding oversight:

- The Deputy Head appoints an official to chair a Director General-level committee (with representatives from each of the Program and Service areas) that is responsible for the review of Preliminary and potential PIAs, as well as for monitoring action plans set by Programs and Services to mitigate the privacy risks of their activities. The Deputy Head approves PIAs following a recommendation of this committee or may ask for more information. PIAs are then forwarded to the OPC.
- Alternatively, a corporate-level committee is established for reviewing PIAs. The committee Chair would be rotated to ensure balanced representation from Program and Service areas. As above, the committee would review PIAs and monitor action plans.
- The institution adopts the practice of encouraging early engagement with the OPC.

For the development of an institutional policy:

- A Director-level committee is established to develop the institution's specific standards and procedures for the conduct of PIAs. Institutional directives are then used by officials to guide implementation of the policy.

For one mid-sized institution:

The conduct of PIAs is integrated into the responsibilities of those who work in the corporate areas of privacy, security and information management. The Privacy Coordinator acts as an advisor to departmental areas that are required to complete PIAs. The Coordinator assists departmental officials by directing them to appropriate TBS guidance and by defining the scope of activities that are required to complete a PIA.

APPENDIX C – Other PIA Audit References and Internet Websites

(**Note**: See Section 5., Closely Related References, for the list of primary sources that may be of assistance when conducting a PIA audit.)

Active Monitoring Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/am-sa/am-sa_e.asp

Access to Information Act
http://laws.justice.gc.ca/en/A-1/8.html

Canadian Charter of Rights and Freedoms
http://laws.justice.gc.ca/en/charter/index.html

Canadian Standards Association Model Code for the Protection of Personal Information
http://www.csa.ca

Government of Canada Security Policy
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

InfoSource
http://www.infosource.gc.ca

Integrated Risk Management Framework
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

National Archives of Canada Act
http://laws.justice.gc.ca/en/N-2.5/index.html

Office of the Privacy Commissioner
http://www.privcom.gc.ca

Official Languages Act
http://laws.justice.gc.ca/en/O-3.01/index.html

Official Languages Policies
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/OffLang/siglist_e.asp

Use of Electronic Networks Policy
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_CP/uen_e.asp

Privacy Impact Assessment
Audit Guide Checklists

The audit checklists should be used to develop audit programs based on the mandate of the engagement and should be focused on areas of highest risk.

Checklist 1: Management Control Framework

Checklist 2: Conducting PIAs

Checklist 3: Notification to the Office of the Privacy Commissioner

Checklist 4: Publication of PIA Summaries

Checklist 5: Implementation and Monitoring of Risk Mitigation Measures

Checklist 6: Performance Assessment

Checklist 7: Compliance-Only Criteria

For easy identification, all mandatory or compliance criteria are shaded in the Checklists.

Checklist No. 1: Management Control Framework

No.	Criteria	Possible Audit Steps	Comments
Management Control Framework **Objective 1:** To identify whether an effective management control framework is in place to support the conduct of PIAs.			
1.1	Objectives and goals of the PIA process are clearly defined, formally approved and effectively communicated.	(a) Determine whether institutional objectives for the PIA process (if developed separate from TBS *PIA Policy* and Guidelines) are defined, verified and approved at an appropriate level. (b) Identify whether specific goals (if established by the institution for implementation of PIA objectives) are clearly defined and approved at an appropriate level. (c) Confirm that PIA objectives and goals are effectively communicated to all key stakeholders in a timely manner.	
1.2	Specific PIA-related accountabilities are established within the institution. (*PIA Policy*, Accountability Sections 1-3)	(a) Verify the Deputy Head formally approves PIAs (i.e. to be provided to the OPC Commissioner). (b) Verify the Deputy Head formally approves final PIAs (i.e. to be published). (c) Check whether the Deputy Head has promoted an awareness of the *PIA Policy* within the institution (e.g. institutional directives, e-mail notifications, annual messages and policy circulations). (d) Verify that the Deputy Head ensures that processes and tools used in assessing privacy impacts are as rigorous as those outlined in the *Privacy Impact Assessment Guidelines*. (e) Confirm that the roles and responsibilities of program and project managers, privacy policy and legal advisors and functional specialists are identified and applied to resolve or mitigate privacy risks.	

No.	Criteria	Possible Audit Steps	Comments
		(f) Confirm that Deputy Heads have established processes for: ▸ Consulting with the OPC; ▸ Responding to any advice that might be offered by the Privacy Commissioner; and ▸ Ensuring that summaries of the results of PIAs are available to the public. (g) Identify whether accountability is formally established for risk mitigation plans and actions implemented as a result of the PIA process. (h) Determine whether consideration has been given to incorporating PIA responsibilities into the accountability accords of affected officials.	
1.3	The organizational structure for the PIA process is formally and effectively supported.	(a) Verify that the organizational structure for the PIA process encompasses all significant stakeholders. (b) Identify whether key privacy, operational and security goals of the organization are readily available. (c) In instances where programs and services use the same or similar approaches to the collection, use and disclosure of personal information, determine whether consideration is given to the development and use of generic assessments. (d) Assess whether a budget(s) is assigned to support the deployment of PIA responsibilities. (e) Determine if the organizational structure for the PIA process supports follow-up and resolution of issues.	
1.4	PIA-related policies, regulations and guidelines are identified, evaluated and incorporated into operational activities.	(a) Confirm whether institutional policies, practices or procedures for the PIA process include requirements and best practices from appropriate policy and regulatory bodies of government (e.g. TBS *Enhanced Management Framework Policy*).	

No.	Criteria	Possible Audit Steps	Comments
		(b) The electronic version of PIAs, PPIAs and associated electronic documents are stored in a central repository of the institution. (c) The central repository for PIAs and PPIAs identifies the location and retention period of hardcopy documents that comprise each PIA and PPIA file.	
1.5	Control activities and mechanisms for the PIA process are in place, relevant, comprehensive and address known risks.	(a) Determine if specific controls over the PIA process are defined, verified and approved at an appropriate level (e.g. verification that minimal information requirements for PIAs have been met). (b) Identify whether PIA process controls are effectively integrated with other processes and practices affecting the PIA.	
1.6	An effective oversight function for the PIA process is in use.	(a) Confirm whether an oversight function exists for the PIA process, and is a component of overall assessment of risk and privacy obligations of the institution. The oversight enables the institution to ensure that programs and activities, subject to a review and that touch on privacy, comply with the privacy principles. (b) Verify that responsibility for oversight of the PIA process is appropriately assigned. (c) Establish whether determinations from the oversight function are communicated in a timely manner within the institution, and to other government bodies (e.g. TBS, OPC) as appropriate. (d) Check that oversight of the PIA process includes internal and/or external audits or evaluations, as appropriate.	

Checklist No. 2: Conducting PIAs

No.	Criteria	Possible Audit Steps	Comments
Conducting PIAs **Objective 2:** To establish whether the institution has formally identified all activities requiring a PIA process and has researched and documented these activities in compliance with *PIA Policy* and *Guidelines*.			
Objective 2.1: To determine if the scope of work required to identify and process a PIA or a PPIA is properly defined.			
2.1.1	PIAs are conducted for proposals for all new programs and services, and for substantially redesigned programs and services, which raise privacy risk. (*PIA Policy*, Section 2)	(a) Verify that institutional practices require initiatives and activities subject to a PIA be reported to a designated official responsible for PIAs. (b) Identify whether institutional practices or policy require responsibility be assigned to coordinate PIA project elements with program/service areas and with outside stakeholders. (c) Determine whether mechanisms are in place to ensure the official responsible for PIAs is apprised of new business, initiatives, services or system initiatives that warrant a PIA. (d) Confirm that the responsible officer formally assesses each institutional initiative to determine the potential applicability of a PIA or PPIA. (e) Verify that for programs and services implemented prior to May 2002, PIAs are conducted where delivery channels have been substantially re-designed or transformed for electronic service delivery in a manner that affects collection, use or disclosure of personal information. (f) Determine if consideration has been given to developing a PIA for existing programs and services where there are outstanding privacy issues.	

No.	Criteria	Possible Audit Steps	Comments
2.1.2	New programs and services, and substantially redesigned programs and services, are defined through a formal Business Case.	(a) Verify whether Business Cases acknowledge the need to assess privacy (and security) risks, if applicable, through the PIA (and TRA) process. (b) Check whether Business Cases identify the PPIA and PIA processes. (c) Establish if Project Work Plans identify a PIA. (d) Assess whether the level of effort, team assignments and completion of project milestones are documented and retained. (e) Determine if project documents identify PIA-related roles and responsibilities of core team members.	
2.1.3	Programs and services identified in PIAs refer to the legislated authority, regulation and policies applicable to the collection, use and disclosure of personal information. (*PIA Policy*, Section 1)	(a) Identify whether programs/services refer to the documented authority for collection, use and disclosure of personal information. (b) Confirm that the authority referenced is current and complete. (c) Verify that PIAs are conducted in consultation with privacy policy advisors. (d) Verify that PIAs are conducted in consultation with legal advisors.	
2.1.4	Responsibility for the PIA process is formally assigned within the affected program/service area.	(a) Check whether institutional practices or policy direct the assigning of a responsible official, within the affected program or service area, to conduct a PIA. (b) Confirm that responsibility for the PIA process includes PIA planning requirements.	
2.1.5	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. (*PIA Policy*, Section 2)	(a) Verify that PIAs are conducted when the design or re-design of a program or service involves: ▸ A new or increased collection, use or disclosure of personal information, with or without the consent of individuals; ▸ A broadening of target populations;	

No.	Criteria	Possible Audit Steps	Comments
		▸ A shift from direct to indirect collection of personal information; ▸ An expansion of personal information collection for purposes of program integration, program administration or program eligibility; ▸ New data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors; ▸ Development of a new or extended use of common personal identifiers; ▸ Significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information; or ▸ The contracting out or devolution of a program or service to another level of government or the private sector. (b) Check whether the PIA scope identifies what part(s) of the program, service or activity will be subject to a PIA. (c) Determine if a PIA Project Plan, Project Schedule, Project Budget and assignment of resources are completed at the early stages of a PIA. (d) Assess whether specific advice and guidance to responsible program/service officers on PIA project plans, schedules, resourcing and budgeting is provided through institutional guidance or TBS *PIA Policy* and Guidelines.	

Checklist No. 2: Conducting PIAs

No.	Criteria	Possible Audit Steps	Comments
Conducting PIAs **Objective 2:** To establish whether the institution has formally identified all activities requiring a PIA process and has researched and documented these activities in compliance with *PIA Policy* and *Guidelines*.			
Objective 2.2: To determine whether business processes subject to a PIA or PPIA are documented sufficiently to support the requirements of the PIA process.			
2.2.1	Guidelines are available directing Programs and Services, subject to a PIA, on how to document business processes.	(a) Determine if documentation of business processes follows a standard set by the department/branch. (b) Identify whether business processes are documented from a summary or 'high' level, down to a level that identifies each data element being processed. (c) Identify whether institutional practices require that PIA documents notifying the OPC include: ▸ An outline of the proposal involving the use of personal information; ▸ Legal authority; ▸ Justification of the proposal; ▸ Stakeholders; ▸ Relevant legislation and policies; ▸ Privacy risks and an analysis of risk mitigation; and ▸ Communications strategy. (d) Confirm that completed business process flow documentation is to be formally approved and dated by the responsible officer. (e) Determine if support for the PIA, or membership in the PIA Team, is provided by the ATIP and the Legal Services Functions, or by persons with related skills and experience.	

No.	Criteria	Possible Audit Steps	Comments
2.2.2	Responsibility for the management of business processes and the flow of personal information is identified and documented.	(a) Verify that management responsibility for a new or modified business processes is identified and formally documented. (b) Establish if personal information definitions are clearly documented. (c) Assess whether legal authorities and references for each collection, use and disclosure of personal information are formally documented (i.e. personal information collected is directly related to an operating program or activity). (d) Determine if all collection, use and disclosure of personal information are formally documented.	
2.2.3	Institutions identify all personal information found within business processes. (*PIA Policy*, Section 3)	(a) Identify if specific features such as the major components of the business processes, as well as how personal information is collected, used and disclosed, are formally documented. (b) Confirm that planned access by the public to information, where that information contains personal information to be excluded from public access, is clearly identified. (c) Verify that Business Process Diagrams (BPDs) provide a detailed description and analysis of the data flows including: data flow tables and systems and infrastructure architectures. (d) Establish if relationships between new or enhanced programs/services and privacy risk, are sufficiently documented to assess privacy risk for each data element, or groups of elements, as applicable. (e) Determine if personal information collection and flow in BPDs are approved by the privacy governance body of the institution.	

No.	Criteria	Possible Audit Steps	Comments
2.2.4	The relationship between personal information and other types of information (e.g. business confidential information) is assessed.	(a) Identify and obtain documentation where personal information is shared or linked with non-personal information in other processes or systems. (b) Where personal information is shared or linked to non-personal information, determine if the level of data protection is appropriately adjusted.	
2.2.5	Outcomes from relevant TRAs or TRA updates are identified and appropriately applied.	(a) Identify whether PIAs identify and record if a TRA or TRA update has been considered, why a TRA was completed or not, and the results of a completed TRA. (b) Confirm that a completed TRA or TRA update is formally added to the PIA file. (c) Verify whether PIA analysis links privacy risks to specific (program or system) design elements. (d) Check that the Privacy Coordinator or Information Management/Information Technology officer provides information on the requirement and use of a TRA to the position responsible for completing the PIA. (e) Confirm that where a TRA(s) has been completed, the Privacy Coordinator or Program officer formally clarifies and confirms privacy related security issues with responsible security personnel. (f) Verify that where a TRA identifies privacy related security issues, the systems infrastructure and architecture(s), the level of physical and logical separation of personal information, and security mechanisms are clearly defined.	

No.	Criteria	Possible Audit Steps	Comments
2.2.6	PIA reports include the minimum required information. (*PIA Policy*, Section 5)	(a) Verify that institutional practices require that a PIA Report include, at a minimum: ▸ an outline of the proposal involving the collection, use or disclosure of personal information and its objectives, including the legal authority and the justification for the proposal; ▸ a list of stakeholders and their roles and responsibilities; ▸ a list of relevant legislation and policies that have implications for privacy and the protection of personal information; ▸ a description of privacy risks that have been identified; ▸ an analysis of options considered to resolve or mitigate privacy risks; ▸ a list of residual risks that cannot be resolved by means of the proposed options and an analysis of possible implications of these risks in terms of public reaction and program success; ▸ action plans to address outstanding privacy risks; and ▸ a communications strategy, where appropriate, to deal with public concerns and perceptions about privacy. (b) Check that documents forwarded to the OPC meet the above-noted requirements of the *PIA Policy* and of the institution.	

Checklist No. 3: Notification to the Office of the Privacy Commissioner

No.	Criteria	Possible Audit Steps	Comments
Notification to the Office of the Privacy Commissioner **Objective 3:** To determine whether the institution's notification to the OPC complies with the *PIA Policy*.			
3.1	Institutional practices require that final PIAs are formally approved by the institution's Deputy Head, and sent to the OPC prior to implementation of new activities. (*PIA Policy*, Section 7)	(a) Verify that institutional practices direct responsible officials to submit approved PIAs at a reasonably early stage (i.e. 6-8 weeks) prior to implementing the initiative, program or service. (b) Confirm that early notification occurs in compliance with *PIA Policy* and institutional practices. (c) Verify that the Deputy Head formally approves PIAs.	
3.2	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.	(a) Establish whether institutional practices identify the requirement for notification to the OPC to review PIAs signed by the Deputy Head. (b) Determine if institutional practices require that OPC comments on PIAs be communicated to the responsible program or service area. (c) Identify whether the role of the OPC and Deputy Head in the final PIA approval/review process is explained in institutional guidance documents.	
3.3	Documents supporting the completion of PIAs are made available to the OPC.	(a) Verify that the requirement to provide PIA-associated documentation to the OPC is documented in institutional practices, including the minimum documentation required and the requirement for any specific documents. (b) Check whether PIA practices identify the need to maintain records of all associated documents, as well as controls necessary for effective document management (e.g. retrieving the documents when required).	

No.	Criteria	Possible Audit Steps	Comments
		(c) Check whether modifications to PIA documents, based on OPC comments, is identified and documented. (d) Determine whether Memoranda of Understanding (MOUs) and Information Sharing Agreements, where applicable, are included in PIA documentation. (e) Establish if Program/Service Action Plans addressing privacy risks (i.e. including mitigation measures and target completion date) are shared with the OPC.	
3.4	All formal OPC responses to institutional requests for PIA information, as well as institutional replies to the OPC, are formally retained by the institution.	(a) Assess whether the requirement to retain records of communication with the OPC is clearly and formally documented in institutional practices or procedures, including the requirement for any specific documents. (b) Determine if the format, means and process for retaining and filing records of communication with the OPC are identified. (c) Identify whether documents for retention include: ▸ Communications from the OPC ▸ The institution's responses to the OPC; ▸ PIA background files; ▸ MOUs; ▸ TRAs; and ▸ information sharing agreements.	

Checklist No. 4: Publication of PIA Summaries

No.	Criteria	Possible Audit Steps	Comments
Publication of PIA Summaries **Objective 4:** To establish whether institutions publish final PIA summaries in compliance with the *PIA Policy*.			
4.1	Final PIA summaries are clearly written in both official languages. (*PIA Policy*, Section 7)	(a) Verify that final PIA summaries are easy to read and understand. (b) Ensure that summaries adequately represent the findings and conclusions from the PIA assessment. (c) Confirm that final PIA summaries are available in English and in French. (d) Check that final PIA summaries provide the same information in French and in English.	
4.2	PIA summaries undergo ATIP review prior to publication.	(a) Determine if draft PIA summaries are reviewed by ATIP (i.e. for potential exemptions), prior to publication, as a formal and required step in the PIA process. (b) Check whether final PIA summaries do not disclose specific security or sensitive information.	
4.3	Draft PIA summaries are forwarded for review to the responsible communications function prior to publication.	(a) Confirm that draft PIA summaries are forwarded for review to the institution's communications function, prior to publication, as a formal and required step in the PIA process. (b) Verify whether the communications function assesses the draft PIA for plain language.	
4.4	Final PIA summaries are readily accessible within the institution and to the public.	(a) Establish that final PIA summaries in French and in English are made available at the same time. (b) Assess whether posting of PIA summaries follows a formally approved institutional plan, where applicable.	

No.	Criteria	Possible Audit Steps	Comments
		(c) Determine if PIA summaries on internal programs or services for employees are posted on the institutional intranet and are available through a means and format that is accessible to all members of the institution (e.g. e-mail, print, database, data warehouse). (d) Identify whether PIA summaries intended for audiences outside the Government of Canada are posted on the institutional Internet site and are available through another means and format that is accessible to all members of the public (e.g. e-mail, print).	
4.5	Final PIA summaries are made available to the public in a timely manner. (*PIA Policy*, Section 7)	(a) Confirm that final PIA summaries are published, in English and in French, in a timely manner. (b) Verify that final PIA summaries follow the institution's publication schedule, where applicable.	

Checklist No. 5: Implementation and Monitoring of Risk Mitigation Measures

No.	Criteria	Possible Audit Steps	Comments
PIA Risk Resolution and Mitigation Measures **Objective 5:** To determine whether risks identified from the PIA process are sufficiently mitigated.			
5.1	Risk evaluation, implications and possible mitigation or resolution recommendations are identified and documented as part of the PIA process. (*PIA Policy*, Section 5)	(a) Identify if PIA risk assessment and mitigation requirements are clearly and formally documented as part of the institution's PIA process. (b) Determine if the risk assessment and mitigation process identifies clear roles and responsibilities for officers on the PIA review committee and for staff of programs or services impacted by a PIA. (c) Confirm that evaluation of privacy risks is documented in each PIA, including the implications of those risks and possible remedies, options and recommendations to resolve or mitigate the risks.	
5.2	Functional specialists addressing PIA risks identify early awareness and knowledge of common risks associated with changes to program or service delivery.	(a) Determine if common privacy risks associated with improvements to service delivery are explained to affected Program/Service officers as an introduction to the development of a risk analysis. (b) Establish whether PIA procedures and practices address industry-recognized risks (e.g. systems weaknesses). (c) Assess whether briefings on risks for affected Program/Service officers include consent management, incremental reduction in privacy rights, data matching, data profiling and function creep, as applicable. (d) Determine whether risk-limiting strategies are explained in the event of cross-jurisdictional PIAs (Questionnaire B) or federal programs and services PIAs (Questionnaire A).	

No.	Criteria	Possible Audit Steps	Comments
5.3	Business processes and data flow tables are documented in support of risk identification and assessment.	(a) Verify whether complete and current business process documentation and data flow tables are identified as a formal input to the PIA process. (b) Identify if completed business and data flow tables are signed-off by responsible subject matter experts. (c) Check that complete and current business process documentation and data flow tables are used to assess risk, where applicable. (d) Establish whether business process documentation and data flow tables used in assessing risk are retained as corporate records in the main PIA file.	
5.4	Risks identified at the branch, function or institutional levels are escalated, as appropriate.	(a) Determine if major risks to branch, function or institutional operations are formally escalated to the appropriate Continuous Risk Management function within the institution. (b) Verify that major risks are addressed in a manner consistent with the institution's Integrated Risk Management practices.	
5.5	Privacy analysis adheres to, and documents, the privacy principles* and applicable legislation and policies. (*PIA Policy*, Section 4)	(a) Verify that PIAs document analysis of the privacy principles and applicable legislation and policy. (b) Determine whether a common or generic approach to PIAs is used to achieve efficiency (i.e. analysis of the same area/topic is not unknowingly repeated). (c) Verify that PIA compliance to the privacy principles*, and to applicable legislation and policy, are documented. * The privacy principles are enumerated in the "Code of Fair Information Practices" in the federal *Privacy Act* as well as in the ten privacy principles attached to the *Personal Information Protection and Electronic Documents Act*.	

No.	Criteria	Possible Audit Steps	Comments
5.6	PIAs are maintained so that privacy risks are identified and then resolved, mitigated or identified as unresolved. (*PIA Policy*, Sections 1 and 4)	(a) Confirm that PIA reports identify privacy risks and options considered to resolve or mitigate privacy risks. (b) Verify that PIA reports also identify, where applicable, residual risk (i.e. risks that cannot be resolved by means of the proposed options and, therefore, serve as early warning that these risks require alternate resolution) and analysis of possible implications of residual risks in terms of public reaction and program success. (c) Determine whether PIAs are maintained on a periodic basis, or as required.	
5.7	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 Policy*, Section 6)	(a) Check if PIA reports clearly provide assurance that no privacy risks associated with program or service delivery activities have been identified. (b) Confirm that where PIAs provide assurance that there are no privacy risks, this conclusion is substantiated with a summary of the risk assessments undertaken. (c) Verify that where PIAs identify privacy risks, the PIA reports clearly identify those privacy risks that require resolution. (d) Determine if significant privacy risks are formally escalated to the appropriate level of management in a timely manner.	
5.8	PIA risk mitigation action plans are formally tracked and results are reported to management.	(a) Identify whether risk mitigation action plans resulting from PIAs are formally prepared and monitored. (b) Confirm that the impact of risk mitigation action plans is independently reported to an appropriate level of management.	

Checklist No. 6: Performance Assessment

No.	Criteria	Possible Audit Steps	Comments
Performance Assessment **Objective 6:** To establish whether performance monitoring is effectively conducted on key financial, operational and human resource aspects of PIA operations in the institution.			
6.1	Operational performance expectations and results for PIAs are reported to management.	(a) Identify whether operational performance expectations and indicators are clearly and formally established. (b) Determine if operational performance indicators are assessed, as required, to ensure their ongoing appropriateness. (c) Assess whether operational performance information is readily accessible and assessable. (d) Check whether operational performance results are reported to an appropriate level of management. (e) Establish if the frequency of reporting supports management decision making.	
6.2	Financial performance expectations and results for PIAs are reported to management.	(a) Determine if the full cost of PIA operations is identified on an annual basis. (b) Identify whether the requirement and justification to cost each PIA and PPIA (i.e. fully identify and cost PIA components), or related groupings of cost, is formally identified. (c) Confirm that financial performance indicators are assessed, as required, to ensure their ongoing appropriateness. (d) Check whether financial performance information is readily accessible and assessable. (e) Verify that financial performance results are reported to an appropriate level of management. (f) Assess whether the frequency of reporting supports management decision making.	

No.	Criteria	Possible Audit Steps	Comments
6.3	Integrated financial and operational performance reporting for PIAs is developed and reported to management.	(a) Determine if the requirements for integrated operational and financial reporting of the PIA process is clearly and formally identified. (b) Check that integrated reporting addresses management needs and reflects 'good reporting practices' identified in other institutions, as appropriate. (c) Confirm that integrated reporting includes analysis of key measures and/or controls (i.e. using relevant statistical, financial and operational information). (d) Verify whether integrated performance reporting is provided to an appropriate level of management. (e) Confirm that the frequency of reporting supports management decision making.	
6.4	Human resource performance expectations and results for PIAs are developed and reported to management.	(a) Determine if human resource performance expectations and indicators are clearly and formally identified. (b) Identify whether human resource performance expectations and indicators include identification of the level of knowledge and experience required for positions with PIA responsibilities, as appropriate. (c) Confirm that human resource performance indicators are integrated with operational and financial performance indicators, as required. (d) Verify whether human resource performance reporting addresses PIA management needs. (e) Establish that performance results are reported to an appropriate level of management. (f) Assess whether the frequency of reporting supports management decision making.	

Checklist No. 7: Compliance-Only Criteria

No.	Compliance Criteria	References	Comments
Compliance-Only Criteria **Objective 7:** To determine if a particular PIA is in compliance with the *PIA Policy*.			
7.1	Specific PIA-related accountabilities are established within the institution. (*PIA Policy*, Sections 1-3)	Criterion 1.2	
7.2	PIAs are conducted for proposals for all new programs and services, and for substantially redesigned programs and services, which raise privacy risk. (*PIA Policy*, Section 2)	Criterion 2.1.1	
7.3	Programs and services identified in PIAs refer to the legislated authority, regulation and policies applicable to the collection, use and disclosure of personal information. (*PIA Policy*, Section 1)	Criterion 2.1.3	
7.4	Initiation and definition of the scope of PIAs are completed in the early stages of the design or re-design of the program or service. (*PIA Policy*, Section 2)	Criterion 2.1.5	
7.5	Institutions identify all personal information found within business processes. (*PIA Policy*, Section 3)	Criterion 2.2.3	
7.6	PIA reports include the minimum required information. (*PIA Policy*, Section 5)	Criterion 2.2.6	
7.7	Institutional practices require that PIAs are formally approved by the institution's Deputy Head, and sent to the OPC prior to implementation of new activities. (*PIA Policy*, Section 7)	Criterion 3.1	
7.8	Final PIA summaries are clearly written in both official languages. (*PIA Policy*, Section 7)	Criterion 4.1	

No.	Compliance Criteria	References	Comments
7.9	Final PIA summaries are made available to the public in a timely manner. (*PIA Policy*, Section 7	Criterion 4.5	
7.10	Risk evaluation, implications and possible mitigation or resolution recommendations are identified and documented as part of the PIA process. (*PIA Policy*, Section 5)	Criterion 5.1	
7.11	Privacy analysis adheres to, and documents, the privacy principles and applicable legislation and policies. (*PIA Policy*, Section 4)	Criterion 5.5	
7.12	PIAs are maintained so that privacy risks are identified and then resolved, mitigated or identified as unresolved. (*PIA Policy*, Sections 1 and 4)	Criterion 5.6	
7.13	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 Policy*, Section 6)	Criterion 5.7	