# Privacy Impact Assessment Template

## Section A: Program or activity information

### 1. Institution and program or activity

Name of institution:

Name of program or activity:

### 2. Multi-institutional program or activity (if applicable)

**Appoint a lead institution with overall responsibility for privacy considerations to help reduce gaps and inconsistencies.**

Lead institution:

Branch:

Directorate:

### 3. Officials responsible for completion of the assessment

**Identify the executive responsible for the program or activity.**

Name:

Title:

Email:

Telephone:

**Delegated privacy official**

Name:

Title:

Email:

Telephone:

For a multi-institutional privacy impact assessment, provide the contact information of the officials of the lead institution. The lead institution will have overall responsibility for privacy considerations to help reduce gaps and inconsistencies.

### 4. Program or activity description

Provide a brief description of the program or activity that includes:

* a high-level description (including the purpose of the program or activity)
* a timeline for implementation
* a description of any changes to the program or activity in the event of a modification to a program or activity

[Insert text here]

### 5. Program or activity scope

Provide an outline of what is in scope and of out scope of the program or activity:

[Insert text here]

## Section B: Notification and personal information

Engage your ATIP or Privacy office to complete the following section.

### 1. Notification

Have the Office of the Privacy Commissioner (OPC) ([SCG-GA@priv.gc.ca](mailto:SCG-GA@priv.gc.ca)) and the Treasury Board Secretariat (TBS) ([ippd-dpiprp@tbs-sct.gc.ca](mailto:ippd-dpiprp@tbs-sct.gc.ca)) been notified of your program or activity (referred to in this section as “program”)? Enter Yes or No:

If No, provide a timeline for when the OPC and TBS will be notified:

[Insert text here]

### 2. Legal authority

1. List the legal authority to collect personal information, citing the relevant clause(s):
   1. If legal authority has not yet come into force, list the proposed legal authority to be in force before collection:
2. If personal information for your program is collected by another government institution, another jurisdiction, or private sector third party and subsequently disclosed to your institution:
   1. List your institution’s legal authority to collect the personal information, citing the relevant clause(s):
   2. List the other institution’s legal authority to disclose the personal information, citing the relevant clause(s):
3. If the social insurance number (SIN) is collected:
   1. List the legal and/or policy authority to collect the SIN, citing the relevant clause(s):
   2. Provide the relevant PIB registration numbers or indicate whether a new PIB is being prepared:

### 3. Personal information banks (PIBs)

Answer **Yes** or **No** to the statements below that apply to your program or activity:

1. Do one or more PIBs already exist for this program? Enter Yes or No:
   1. If **Yes**, Provide the PIB registration number(s):

**Note:** Your ATIP or Privacy Office may request to review the current PIBs or the text of the PIBs relied upon.

1. Does a PIB need to be substantially modified or edited for this program? Enter Yes or No:
   1. If **Yes**, provide the registration number or numbers of the PIB or PIBs that need to be substantially modified or edited and explain what modifications need to be done:

[Insert text here]

**And**

b) Update the PIB using the Personal Information Bank Submission Form.

1. Does a new PIB need to be prepared for this program? Enter Yes or No:
   1. If **Yes**, prepare a new PIB using the Personal Information Bank Submission Form.

### 4. Handling of personal information

Use the table below to describe the handling of the personal information for both administrative and non-administrative purposes. Describe:

* how the personal information is being created (includes data linking) or collected (directly from the individual, indirectly from another source, or a combination of the two)
* how the personal information will be disclosed: list the entities to whom it will be disclosed and link the disclosure to the purpose of the program
* how the personal information will be used and who will use the information: link the use to the purpose of the program
* how the personal information will be stored and the retention period for the elements of personal information
* how the personal information will be disposed of

This section should also include the identification of partners that handle the personal information during the administration of your program.

| **1. Categories of personal information** | **2. Data Elements** | **3. Created or collected from (source)** | **4. Created or collected by** | **5. Method and format of collection** | **6. Purpose of the collection** | **7. Used by** | **8. Consistent uses\*** | **9. Accessed by** | **10. Disclosed to\*** | **11. Transmission method (how it is disclosed)** | **12. Location of storage and retention period** | **13. Disposed of** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] | [Insert text here] |

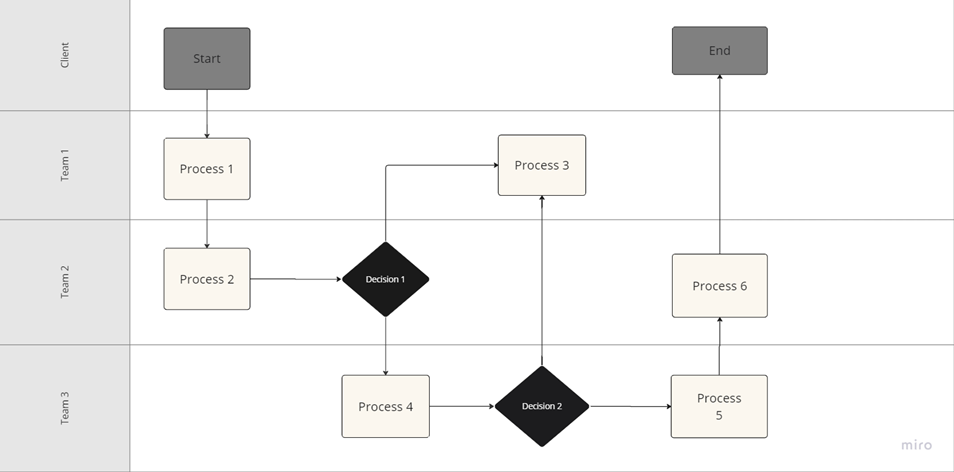
\* Can include disaggregated data used for program monitoring, evaluation and reporting purposes.

### 5. Process flow description

Describe each step of the flow of personal information within the program. The description may be provided using a diagram or text. If a diagram is provided, it must be accompanied by a narrative.

The flow of personal information can be within or outside the institution where other federal institutions or third parties are involved. The process flow should include everything within the scope of the assessment, as outlined in Section 1. The description of the process flow should also include any non-administrative uses of personal information such as reporting, monitoring and evaluation.

1. Process flow diagram (optional): Insert one or more diagrams to illustrate the flow of the personal information within the program. See below for an example of a “swim lane” diagram.



1. Narrative (required): Describe each step of the flow of personal information within the program.

| **Step number** | **Description** |
| --- | --- |
| 1. | [Insert text here] |
| 2. | [Insert text here] |

## Section C: Privacy analysis

**Step 1:** Enter **Yes**, **No** or **Not applicable** for each question below, as appropriate.

**Step 2:** Complete all tables below. Some tables will require engagement with other stakeholders, including third parties, security and cyber security officials, legal services, and contracting or procurement officials.

**Step 3:** Send your answers and completed tables to your ATIP or Privacy Office, which may ask follow-up questions or ask for additional documentation for its review or confirmation.

**Step 4:** Your ATIP or Privacy Office will assess the responses to the questions and may add information in the “Justification” column to substantiate the answer and help assess potential risks and compliance issues.

**Step 5:** Your privacy official will use all the information provided and any requested additional information or documents to determine whether there are any potential risks or compliance issues.

**Step 6:** Collaborate with your privacy official to develop a plan to accept or mitigate risks (see **Section D: Risk Mitigation and Compliance Issue Action Plan**).

### 1. Accountability

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Have you documented who has control of the personal information throughout the program? | Enter Yes or No: | [Insert justification if necessary]  A privacy official may want to review the documentation. | [Insert risk or compliance issue]  Include any risks related to this question, if applicable. See Annex A: Privacy Risk Assessment Grid.  **Example**  There is a risk that in the event of a privacy breach, response times could be prolonged given the absence of clearly defined roles and responsibilities for the overall handling of personal information. |
| 1. Have you documented who is ultimately accountable for the personal information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will any third parties, including private sector third parties, be involved in the program and have access to or responsibility for the personal information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If third parties will be involved, do you have a written record (arrangement, agreement or contract) of understanding in place that establishes privacy requirements? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the institution be provided with the results of regularly scheduled audits and compliance checks on the privacy requirements of all involved parties? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 2. Limiting collection

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Will the personal information collected be directly related to the program? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have you documented the reason(s) for the collection of personal information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are all the personal information categories listed in the relevant personal information bank (PIB)? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will personal information be collected indirectly, meaning from a source other than the individual that the information is about? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the personal information is collected indirectly, will it be collected with consent from the individual? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the personal information will be collected indirectly without consent, is the collection a result of a disclosure under [subsection 8(2) of the *Privacy Act*](https://laws-lois.justice.gc.ca/eng/acts/p-21/FullText.html#:~:text=Disclosure%20of%20personal,the%20information%20relates.)? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the personal information is collected indirectly without consent, will the information be used to make a decision about the individual? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the personal information will be collected indirectly without consent, could direct notification to the individual result in the collection of inaccurate information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the personal information will be collected indirectly without consent, could direct notification of the individual defeat the purpose or prejudice the use for which the information is collected? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will consent require a positive action, that is, a written agreement or signature, by an individual rather than being assumed as a default (implied) consent? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have all efforts been made to minimize the collection of data elements? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there consequences to the individual as the result of a refusal to consent? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there mechanisms to permit individuals to withdraw their consent? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will other federal institutions, other jurisdictions or private sector third parties be collecting personal information on behalf of your institution? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. If yes, will they present the privacy notice at the time of collection? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the program involve collection of personal information through a common client identifier? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there mechanisms in place to ensure that the individual has the capacity to give consent? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Can personal information be collected from a person authorized to act on behalf of the individual? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are standards and mechanisms in place to ensure the recognition of persons authorized to make decisions on behalf of others (for example, a minor or incapacitated person)? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 3. Limiting use

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Will personal information be used exclusively for the reason(s) it was collected? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Do you have processes in place to ensure that personal information will be used only by or disclosed to individuals who have a need to know (including within your institution and any receiving public sector organization or third parties)? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will personal information be used for a purpose that is not identified in the relevant PIB? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the personal information be used for any consistent uses? | Enter Yes or No: | Indicate those uses. | [Insert risk or compliance issue] |
| 1. Will personal information be used for any secondary uses? | Enter Yes or No: | Indicate those uses. | [Insert risk or compliance issue] |
| 1. Will there be any new uses of personal information previously collected that are directly connected to your program’s original purpose? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  Indicate those uses. | [Insert risk or compliance issue] |
| * 1. If yes, could individuals reasonably expect their information to be used for that new purpose? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the personal information be used in a way that involves technology that either assists or replaces the judgment of human decision makers? An example is a system, tool or statistical model that makes an administrative decision or a related assessment about a client, with or without human review. | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If no, indicate why. | [Insert risk or compliance issue] |
| If yes, will you comply or have you complied with the [*Directive on Automated Decision-Making*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592)? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the personal information be used for planning, monitoring and evaluation purposes or for reporting purposes? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If yes, describe what those purposes are. | [Insert risk or compliance issue] |
| 1. Are there safeguards in place to ensure that only personal information needed for these purposes is made available to those with a need to know for their work? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the personal information be used for the training, testing or refinement of artificial intelligence systems? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. If yes, will you comply or have you complied with the Directive on Automated Decision-Making? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will personal information be used for conducting investigations or enforcement activities? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If yes, specify what those activities and legal authorities are. | [Insert risk or compliance issue] |
| 1. Will personal information elements, such as a SIN or any other identifying number or symbol, be used for the purposes of linking across multiple databases? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. When data will be matched for an administrative purpose, will it be consistent with the stated purposes for which the personal information is collected? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there an activity log attached to the personal information record to document uses and disclosures that are not listed in the relevant PIB? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the program result in an increased ability to undertake surveillance or monitoring? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the system, software or program application use any tracking methods, such as cookies, to collect personal information about users and their transactions? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 4. Limiting disclosure

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Will the disclosure of personal information be limited to the purpose of the disclosure? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will personal information be disclosed for a reason or reasons not identified in the relevant PIB? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Has consent been obtained for personal information that will be used or disclosed for a secondary purpose that has not previously been identified in the relevant PIB? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If personal information is disclosed without consent, has the specific authority for the disclosure been identified? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If yes, list the specific authority. | [Insert risk or compliance issue] |
| 1. Will personal information be disclosed with other federal institutions, other jurisdictions or private sector third parties? If so, identify them. | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Do you have an information-sharing agreement (for example, a memorandum of understanding, an accord, an arrangement or a contract) with another federal institution, other jurisdiction, or a private sector or third party? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have formal information-sharing provisions been established on the use, retention, disclosure and safeguarding of personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. Do these provisions include security incident or privacy breach management? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will any identifying number, symbol or other particular assigned to an individual, such as a SIN, be disclosed? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will personal information be disclosed for data-matching purposes? | Enter Yes, No or Not applicable: |  | [Insert risk or compliance issue] |
| 1. Will personal information be used, disclosed or retained outside Canada? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 5. Retention and disposal

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Is there a retention schedule? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  Your ATIP or Privacy Office or information management expert may ask to review the retention schedule.  If you are not sure what your program’s retention schedule is, contact your information management branch.  Indicate whether the retention schedule is in development. | [Insert risk or compliance issue] |
| 1. Are there procedures in place for the disposal of personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there an accurate and up-to-date Records Disposition Authority (RDA) in place? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If you are not sure of your program’s RDA, contact your information management branch.  Indicate whether the retention schedule is in development. | [Insert risk or compliance issue] |

### 6. Accuracy

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Are there procedures to ensure that personal information is as accurate, complete and up to date as possible? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will youensure accuracy through all reasonable steps, including:    1. Through direct collection or validation with the individual? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. By obtaining information from trusted sources (either public or private) and verifying accuracy against existing personal information before use? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. With a personal information matching program to verify personal information against a trusted source where authorized or where consent was obtained? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there a process in place for correcting inaccurate information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will third parties to whom personal information has been disclosed, be notified (automatically or not, through procedures in place) of changes to those records? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  If yes, explain how. | [Insert risk or compliance issue] |
| 1. Are there processes or protocols in place to monitor changes to records of personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. If yes, does the record indicate the changes made and the date of each change? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is a record kept regarding:    1. Requests for a review of errors or omissions? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. Corrections or decisions to not correct? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Do you ensure accuracy by technological means to identify keystroke errors and discrepancies? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there documented procedures for how to respond to requests to correct personal information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are systems designed to ensure that an individual has been notified that a correction has been made to their information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 7. Safeguards

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Will privacy training be provided to employees? | Enter Yes or No: | [Insert justification if necessary]  Include whether this training occurs only once or is repeated regularly, for example, every two or five years. | [Insert risk or compliance issue] |
| * 1. If yes, is there specialized training provided for this specific program? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  Your ATIP or Privacy Office or security expert may ask to review any related documentation or a brief description of the procedures. | [Insert risk or compliance issue] |
| 1. Have all required Authorities to Operate (ATOs) been granted? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If the ATO was granted “with conditions,” is there a mitigation plan in place and a timeline for completion? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  The mitigation plan, including timelines for completion, may be requested for review. | [Insert risk or compliance issue] |
| 1. Have all security assessments, authorizations, threat and risk assessments, or their equivalents, been completed in consultation with the departmental information management or information technology security team? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  A summary of the assessments and risks identified may be requested for review. | [Insert risk or compliance issue] |
| 1. Will controls be in place for all processes to grant authorization to modify (add, view, change or delete) personal information from records, upon implementation? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will security measures be in place to match the sensitivity of the information recorded, upon implementation? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will the program use specialized software or new databases? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there guidelines, policies or training materials for employees who handle personal information that go beyond the requirements of the [*Directive on Personal Information Requests and Correction of Personal Information*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32590)? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Can the systems track and record who accesses, changes or discloses personal information, along with the date it happened? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. If yes, are access, changes and disclosures logged and monitored? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there a plan for quality assurance and auditing of programs to assess the system’s safeguards to make sure they are working properly? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there policies and procedures in place to manage the use of portable storage devices such as flash drives that store personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will user accounts, access rights and security authorizations be controlled by a system or record management process? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will access rights be provided to users only on a need-to-know basis, consistent with the stated purpose for which the personal information was collected? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Does your institution have a privacy breach response plan in place? (see the [*Directive on Privacy Practices*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18309)) | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there contingency plans and documented procedures in place to identify and respond to privacy breaches? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there documented procedures in place to communicate privacy breaches to:  * the affected individual? * law enforcement authorities? * relevant program managers? * affected third parties, including other federal institutions? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there procedures in place to remove or modify user access rights when job responsibilities change? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there security controls in place for remote access and the use of mobile devices? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 8. Openness

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Will a summary of the PIA be published online, using the Summary of the Privacy Impact Assessment template? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Do you have a privacy notice to notify individuals of the collection of their personal information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Does your privacy notice include all of the following elements:  * the purpose and legal authority for the collection * any uses or disclosures that are consistent with the original purpose * the relevant PIB description * any legal or administrative consequences for refusing to provide the personal information * the rights of access to, correction of and protection of personal information under the *Privacy Act* * the right to file a complaint with the Privacy Commissioner of Canada | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Has the privacy notice been adapted for verbal communication at the time of collection? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| * 1. If yes, has a text been developed? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is the privacy notice available and consistent across all media and platforms of collection (that is, phone, paper and online)? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there a clearly defined and easy process for individuals to communicate with the appropriate individuals regarding the handling of their personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Is there a communications plan to explain to the public how personal information will be handled and protected? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### 9. Individual access

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Are systems designed to ensure that an individual can have access to their personal information, including all other programs or applications that have received copies of the information? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are all custodians aware of the process related to an individual’s right of access (that is, through privacy notices and PIBs)? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are there documented procedures developed or planned on how to initiate informal and formal personal information requests? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If appropriate, are individuals provided with access to their personal information in the official language of their choice? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. If appropriate, will individuals be provided with access to their personal information in alternative formats? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Has consideration been given to providing individuals “routine” or informal access to their personal information? | Enter Yes, No or Not applicable: | [Insert justification if necessary]  Describe such access. | [Insert risk or compliance issue] |

### 10. Challenging compliance

| **Question** | **Answer** | **Justification (if necessary)** | **Risk or compliance issue (to be completed by privacy officials on receipt)** |
| --- | --- | --- | --- |
| 1. Is there a process to receive and respond to privacy-related complaints and questions? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are the complaint procedures for the proposed program in line with legislative and policy requirements? | Enter Yes or No: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Are all those who will have access to and handle personal information aware of an individual’s right of access and complaint process? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Has a procedure been established to log and periodically review the nature, frequency and resolution of privacy-related complaints? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Will there be oversight and review mechanisms to ensure compliance with legislative and policy requirements? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have you documented who is responsible for receiving and resolving privacy complaints? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |
| 1. Have oversight agencies, including the OPC, issued reports or opinions on issues that would be relevant to the program? | Enter Yes, No or Not applicable: | [Insert justification if necessary] | [Insert risk or compliance issue] |

### Data-Matching Table (if applicable)

| **Name of activity** | **Description of activity** | **Purpose of activity** |
| --- | --- | --- |
| [Insert name of activity] | Describe how one data element or a group of data elements will be matched to another data element(s) in another system or database. Such a match can occur automatically between systems or manually and involve a name, date of birth and unique identifier matched against a registry.  Has your program considered the applicability of the [*Directive on Automated Decision-Making*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592) if the data matching is involved in an administrative decision? | Identify the reason behind this data matching (for example, to confirm identity). |

### Information Technology Solutions Table (if applicable)

| **Name of information technology (IT) solution** | **Purpose of IT solution** | **Business owner** | **Security assessment reports completed** |
| --- | --- | --- | --- |
| [Insert the name of the IT solution] | Identify the reason for the use of the system and describe how it will be used. | Identify the business owner, that is, who is accountable for the system or solution. | List any security assessments and authority to operate or other security-related assessments that has been or is being conducted and any residual risks related the privacy and the protection of personal information. |

### Access Inventory Table

Inventory of individuals or groups who have access to and handle personal information (under your institution’s control).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Branch or division** | **Position or titles** | **Rationale for access** | **Number of users** | **Geographical location (of the individuals or groups and the personal information, if in a different location)** |
| [Insert branch or division] | [Insert position or titles] | Describe the reason(s) why this individual or group needs access. | Insert the number of users with access  Try to be as precise as possible, but you can provide a range instead of an exact number for larger groups | Insert geographical location |

## Section D: Risk Mitigation and Compliance Issue Action Plan

### Risk Mitigation Action Plan

**Step 1:** In the “Risk description” column, identify, summarize and contextualize the risks that were identified by answering the questions in [Section C: privacy analysis](#_Section_C:_privacy). These risks may be derived from the “no” answers in that section, but a “No” answer is not always a risk. A “Yes” answer does not preclude a risk.

**Step 2:** In the “Affected privacy principle(s)” column, identify the affected principle following the 10 principles outlined in [Section C: privacy analysis](#_Section_C:_Privacy).

**Step 3:** In the “Risk level” column, identify the risk level. Use either [**Annex A: Privacy Risk Assessment Grid (Non-Mandatory)**](#_Annex_A:_Privacy) or your institution’s own risk assessment methodology to determine the level.

**Step 4:** In the “Mitigation measures” column, determine, with your ATIP or Privacy Office, an appropriate mitigation measure for each risk, including who will be responsible for each and a target completion date.

| **Risk number** | **Risk description** | **Affected privacy principle(s)** | **Risk level** | **Mitigation measures** |
| --- | --- | --- | --- | --- |
| 1 | There is a risk that:  Identify, summarize, describe and contextualize the risk. | The affected privacy principle(s) is or are:  Identify the principles affected, that is, accountability, identifying purposes, and so on | Identify the risk level associated with the risk. | Summarize the planned activities that will be undertaken to mitigate the risk.  Lead:  Target completion date: |

### Compliance Issue Action Plan

**Step 1:** In the “Compliance issue” column, identify, summarize and contextualize the compliance issues that were identified by answering the questions in [Section C: privacy analysis](#_Section_C:_Privacy). These issues may be derived from the “No” answers in that section, but a “No” answer is not always a compliance issue. A “Yes” answer does not preclude a compliance issue.

**Step 2:** In the “Non-compliance type” column, identify the type of non-compliance and cite the relevant clauses of the legislation or policy. Use either [**Annex B: Non-Compliance Grid (Non-Mandatory)**](#_Annex_B:_Non-compliance) or your institution’s own non-compliance type to determine the type.

**Step 3:** In the “Corrective measures” column, determine, with your ATIP or Privacy Office, an appropriate corrective measure for each compliance issue, including who will be responsible for each and a target completion date.

| **Issue number** | **Compliance issue** | **Non-compliance type** | **Corrective measures** |
| --- | --- | --- | --- |
| 1 | Identify and contextualize the compliance issue. | Identify the type of non-compliance and cite the relevant clause(s) of the legislation or policy:  Law or regulation  Government of Canada policy  Internal policy | Summarize the planned activities that will be undertaken to ensure compliance.  Lead:  Target completion date: |

## Section E: Formal approvals

**Sign off by the program area**

The following signature represents a commitment to comply with the *Privacy Act* and privacy policy requirements as they relate to the administration of this program or activity and addressing the risks as part of the mitigation action plan.

Signature:

Date:

[Name, position title of official responsible for the program or activity (for example, Director General)

Name of directorate

Name of branch]

**Sign-off for the section 10 of the *Privacy Act***

As head of the institution or as delegate, I approve this assessment and am satisfied that privacy risks have been identified and will be mitigated according to the action plan as they relate to the administration of this program or activity.

Signature:

Date:

[Name, position title of official responsible for the program or activity (for example, Director General)

Name of directorate

Name of branch]

**Note:** If the program or activity involves more than one institution, the signatures of the official responsible for the program or activity and the signature of the section 10 official for each institution must be provided.

## Annex A: Privacy Risk Assessment Grid (Non-Mandatory)

The privacy risk assessment grid in this annex is a non-mandatory tool that can be used to determine the impact of a privacy risk identified during the privacy analysis and the likelihood of the risk occurring. Privacy officials are encouraged to adapt the tools to the needs of their institutions. If you use the grid, follow the steps below.

Step 1: Determine the potential impact (to the individual or institution) of the risk should it occur, based on the scale below.

Step 2: Scroll down to the “Impact” column and determine the likelihood of the risk occurring (unlikely, likely, very likely, almost certain).

Step 3: The area in the scale where the level of impact and level of likelihood intersect indicates the level of risk.

Example: A potential asset loss for the institution of $2 million (impact level of 2) that is very likely (likelihood level of 2) to occur under standard circumstances will result in a medium risk (2 + 2 = 4).

Step 4: Repeat for every risk identified in [Section C: privacy analysis](#_Section_C:_privacy).

Note: Although it is strongly recommended to use as much evidence as you have at your disposal to objectively complete the assessment, for example, potential days of service disruption (based on previous events), it is important to note than some subjectivity in the assessment and result is expected.

### Privacy Risk Assessment Grid (non-mandatory)

| **Type of harm** | **Negligible: 0** | **Low: 1** | **Medium: 2** | **High: 3** | **Definitions of impact types** |
| --- | --- | --- | --- | --- | --- |
| **Physical security and financial harm to individuals** | Negligible impact; inconvenience | Minimal or short-term injury and/or financial losses that would have a minimal impact on individuals | Long-term injuryand/orfinanciallossesthat would have a moderate, short-term impact onindividuals | Serious and irreversible injury or financial losses that would have a substantial and long-termimpact on individuals | Harm to the security of individualscanbeinthe formofphysicalinjury.  Financialharmcanbe intheformofnon-recoverable financial losses orassetlosses. |
| **Psychological harm to individuals** | Discomfort | Negligible psychologicaldistress that does not requireprofessionalattention | Short-term psychologicaldistress that interferes with thedaily activities of anindividualand thatcould beaddressedwith professionalattention | Long**-**term psychologicaldistress that interferes with thedaily activities of anindividualand thatwould requirelong-term professionalattention | Psychological harm can beexperienced in different forms, suchas difficulty concentrating, sadness,anxiety,depressionand so on. |
| **Reputational harm to individuals** | Inconvenience | Reputational harm thatwould have negligibleimpactontheindividual | Short-termreputational harmthat would have anoticeable impact ontheindividual | Long-termreputationalharmthat would haveseriousimpactsontheindividual | Reputational harm to an individualcan be in the form of publicdiscomfort, embarrassment, loss ofrespect, social dilemma, characterdegradation,ignominyorsocial isolation. |
| **Financial resources or assets loss for the institution or institutions** | Upto$100,000 | $100,000 to $1 million | $1 million to $5 million | $15 million | Financialharmcanbeintheformof non-recoverablefinanciallossesor assetlosses. |
| **Operations and capacity to deliver programs or services for the institutions** | Consequences can be dealt with through normal activity with no service interruption | Consequences threaten the efficiency or effectiveness of some parts of the program but can bemanagedinternally; can result in very short-term service interruption (one day to one week) | Consequencescouldcausesignificantreviewor change inthe administration ofthe program that could result in service interruption of up to six months | Consequences threaten the survival of the program and requireinterventionbysenior managementor electedrepresentatives, and can result in long-term service interruption | Impacttothe programoperationscouldbeinthe formofdisruptions,delaysorinterruptionsinproviding servicestoclients. |
| **Reputation and relationships for institutions with stakeholders** | No damage to therelationship, no dissatisfaction from clients or the public, and no unfavourable media attention | Setback in client trust**,** noticeable increase in client complaints, and unfavourable mediaattention | Publictrustandconfidenceintheprogramor servicearenegativelyaffectedpotentiallysubjecttonegativecriticismby a central agency ortheOffice of the Privacy Commissioner | Significant loss of public trust**,** embarrassment forthe institution**,** subject to an auditor investigationby the Office of the Privacy Commissioner, or strongcriticism bycentral agency or scrutiny by a parliamentary committee | Reputationalimpactscouldbeintheformofcriticism,unfavourablemediaattention or loss of public trusttowardinstitutions, **or** publicembarrassmentofministersorseniorofficials. |

### Likelihood scale

| **Likelihood of harm occurring** | **Negligible: 0** | **Low: 1** | **Medium: 2** | **High: 3** | **Risk rating** |
| --- | --- | --- | --- | --- | --- |
| **Almost certain:** Occurs continuously;shouldoccurunder typicalcircumstances | 3 | 4 | 5 | 6 | High (5 to 6) |
| **Very likely:** Occurs frequently; couldoccur under standardcircumstances | 2 | 3 | 4 | 5 | Medium (3 to 4) |
| **Likely:** Occurs occasionally; could occurunderlimited circumstances | 1 | 2 | 3 | 4 | Low (2 to 3) |
| **Unlikely:** Occurs infrequently; couldoccurunder exceptional circumstances | 0 | 1 | 2 | 3 | Negligible (0 to 1) |

## Annex B: Non-compliance Grid (non-mandatory)

The non-compliance grid is a non-mandatory tool that can be used to determine compliance issues and the level of non-compliance.Privacy officials are encouraged to adapt the tools to the needs of their institutions. If you choose to use the grid, follow the steps below.

Step 1: Determine the type of non-compliance based on the grid below (that is, legal, Government of Canada policy, internal policy, and so on)

Step 2: Repeat for every compliance issue identified in [Section C: privacy analysis](#_Section_C:_privacy).

**Non-Compliance Grid**

| **Law or regulation** | **Government of Canada policy** | **Internal policy** |
| --- | --- | --- |
| Non-compliance with Government of Canada Law or regulation (for example, the *Privacy Act*) | Non-compliance with Government of Canada directive, policy instruments or procedural documents (for example, the *Policy on Privacy Protection*, *Directive on Privacy Practices*) | Non-compliance with the institution’s internal directive or policy instruments or procedural documents |