PPIA/PIA Review Criteria

Message from the Commissioner:

Public bodies are entrusted with a large amount of personal information about individuals, especially residents of the province. In many cases, this is information we have to provide to the government in order to obtain a necessary service. Members of the public have a right to expect that public bodies and their employees will treat their personal information with respect and confidentiality.

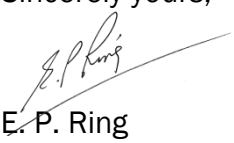
A Privacy Impact Assessment (PIA) is a process meant to assess the impact a project will have on the privacy of individuals. All projects involve risk, and an important part of the PIA process is the identification of risks that personal information may be lost, stolen, disclosed improperly, etc. and the suggestion of corresponding mitigation strategies.

A PIA is a valuable tool to ensure that public bodies are in compliance with the *ATIPPA, 2015*; in addition to legislative requirements to complete PIAs in certain circumstances, a PIA will be instrumental in the event of a privacy breach investigation or as part of the audit process. A robust PIA can show that all risks were identified, considered and appropriately mitigated.

At its core, a PIA documents the information handling practices of the public body, describing the information collected, detailing who has access and what they can do with this access, outlining how the information flows and documenting the reason for the collection.

The OIPC has reasonable expectations. Public bodies may complete a preliminary privacy impact assessment (PPIA) and determine that a full PIA is not required; however, the OIPC expects that reasons for this conclusion will be documented and may require that these reasons be provided to it as part of an investigation or audit.

Sincerely yours,



E. P. Ring
Privacy Commissioner

Contact Information:

Office of the Information and Privacy Commissioner
3rd Floor, 2 Canada Drive, Sir Brian Dunfield Building
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Tel: (709) 729-6309 Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
E-mail: commissioner@oipc.nl.ca
www.oipc.nl.ca

Introduction

This guide outlines OIPC expectations regarding a preliminary privacy impact assessment / privacy impact assessment (PPIA/PIA). As many public bodies have already developed PPIA and PIA templates, including the ATIPP Office, this guide is meant to complement existing resources. For any public body that does not have a template, a sample Table of Contents is located in Appendix A – Table of Contents.

Each section provides background information on the topic and then identifies some expectations of the OIPC; these expectations are summarized in Appendix B – Summary of Expectations. Please note that the list of expectations is not exhaustive and expectations may vary depending on the specifics of the project being assessed. For example, a project that collects demographic information (such as name and mailing address) directly from a small number of individuals would not require the same level of detail as a project that collects, from various sources, detailed information on the majority of residents in the province.

Additional information for many sections is provided in the Appendices.

What is a PPIA?
In general, a PPIA or a threshold assessment is conducted to determine if a full PIA needs to be completed. The PPIA covers much of the same content as a PIA, just at a different level of detail. This analysis is an important component of the overall project and, even if it determines that a full PIA is not necessary, may provide helpful commentary on risk mitigation. For example, if a project involves de-identified information, a full PIA report may not be required. However, the PPIA would document why the decision to de-identify the information involved was made in the first place.

For the purpose of this document, PPIAs and PIAs are referred to as PIAs, unless discussing the difference between the two documents. The OIPC expects PPIAs to address the same topics as the PIA; the PPIA will not require the same level of detail.

For the purpose of this document, a project includes, but is not limited to, projects, services, systems, initiatives, and any collection of personal information, including databases and information banks.

What does *ATIPPA, 2015* say about PIAs?

The *ATIPPA, 2015* defines a PIA in section 2(w)

> *2 (w)"privacy impact assessment" means an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act*

Part III of the Act addresses the protection of personal information and establishes requirements for collection, use, disclosure, as well as the ability for individuals to file a privacy complaint.

Section 72 makes PPIA/PIAs mandatory for departments and branches of the executive government:

> *72. (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act*

(a) a privacy impact assessment for that minister's review and comment; or
(b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.

(2) A Minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.

(4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

What the OIPC expects when a public body decides, based on a PPIA, that a full PIA report is not necessary:

The OIPC recognizes that every project does not require a full PIA report; this is one reason that public bodies complete preliminary reviews. If the results of the preliminary review lead the public body to determine that a full PIA Report is not required, the OIPC would expect to see discussion on how this decision was reached. There should also be an established threshold documented in policy or procedure to ensure consistency. Considerations may include, but not be limited to, a combination of factors, including:

- Limited personal information collected; information collected is not sensitive;
- Limited number of individuals impacted by the project;
- Information directly collected for a single stated purpose;
- Personal information is used, but not disclosed.

As the *ATIPPA, 2015* does not define a common or integrated program or service, the OIPC is adopting a definition similar to the one in Schedule 1 of British Columbia's *Freedom of Information and Protection of Privacy Act*. Our definition is:

"common or integrated program or service" means a program or service that
a) provides one or more services through
(i) a public body and one or more other public bodies or agencies working collaboratively, or
(ii) one public body working on behalf of one or more other public bodies or agencies

Please note that, because of its unique role, the involvement of the Office of the Chief Information Officer (OCIO) does not automatically make a project a common or integrated program or service. For example, if the OCIO is developing an IT system on behalf of a public body, the project would not necessarily fall under this definition.

Any public body that is unsure if the PIA subject would be considered a common or integrated program or service should contact the OIPC to discuss. Even if it is not a common or integrated program or service, the OIPC would be pleased to offer assistance by providing feedback on a PIA.

Departments and branches of the executive government should contact the ATIPP Office to discuss their project; the ATIPP Office has also developed a PIA template to assist departments and branches of the executive government in compliance with section 72.

The *ATIPPA, 2015* also expands the authorities of the Office of the Information and Privacy Commissioner. Section 95 of the *ATIPPA, 2015* establishes the general powers and duties of the Commissioner. Public bodies should be aware that this Office has the authority to conduct investigations to ensure compliance with the *ATIPPA, 2015* and to monitor and audit practices and procedures employed in carrying our responsibilities and duties under the *ATIPPA, 2015*. A PIA is a useful tool for public bodies to demonstrate compliance with, or at least consideration of compliance with, the *ATIPPA, 2015*.

OIPC Expectations

The OIPC expects public bodies to be aware of their obligations under the *ATIPPA, 2015*, as well as the authority and mandate of the Commissioner under the *ATIPPA, 2015*.

What is a PIA?

A PIA examines a project in the context of the privacy principles, best practices, codes of conduct, legislation, and relevant directives. A well written PIA identifies the impacts that a project will have on privacy and suggests mitigation activities to lessen the impacts and risks. In general, PIAs should be conducted early enough in the project to allow the findings to be considered in the decision-making process. Even once the project is implemented, the PIA should be revisited if any further changes are proposed, if the overall operating environment changes or as per the review schedule established in the document. PIAs should be conducted for existing projects as resources allow.

In general, PIAs should be written in an easily understandable format. It should not contain jargon or project specific acronyms. The purpose of the PIA process is to identify privacy risks and identify mitigation activities; it is not meant to be a marketing tool that only shows the benefits of the project.

> *A PIA is a systemic process that identifies and evaluates, from the perspective of all stakeholders, the potential effects on privacy of a project, initiative, or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts*
> *Roger Clarke, An evaluation of PIA guidance documents. International Data Privacy Law*

OIPC Expectations

Public bodies should be aware of what a PIA is, when a PIA should be conducted, the resources available and the benefits of conducting a PIA. Any PIA sent to the OIPC for review, either as part of the PIA review process or other investigation, should be understandable. If the PIA references a document, the document should either be summarized or attached as an appendix; if the document is publicly available, a link to the document is sufficient.

When should I complete a PIA?

It is best practice to complete a PIA on any project that collects, uses or discloses personal information, be it in the development stage or even fully implemented.

While not an exhaustive list, some common triggers for a PIA include:

- A new way of doing things (for example, converting from paper files to an electronic system)
- Databases (merging existing databases, adding indirectly collected information to an existing database, etc)

- New safeguards or threats, or changes to the overall security safeguards used to manage and control access
- New collections, uses or disclosures, with or without consent of the individual
- Shift from direct to indirect collection
- Increased sharing of personal information between programs or public bodies
- Contracting out or use of third parties
- A broadening of the target population
- Anything that has a privacy implication, including legislation and policies

OIPC Expectations

Any project that collects, uses or discloses personal information should have documentation assessing the impact the project has on an individual's privacy. Such documentation may be in a PPIA, PIA, risk assessment, etc.

While some organizations believe that PPIAs and PIAs need only be done on new or re-designed projects, it is best practice to complete PIAs on all projects, including current projects. All public bodies need to comply with the *ATIPPA, 2015* and a PIA is one tool that is helpful in ensuring compliance.

The OIPC would expect public bodies to document when a PIA should be considered and, if preliminary assessments are conducted, the analysis and documentation required if it is determined a full PIA report is not required.

Content

As many public bodies have established PIA templates, including the ATIPP Office, the OIPC chose not to release a template. Instead, this Office has focused on the content the OIPC expects to be considered during the PIA process. While a PPIA would not contain the same level of detail as a full PIA report, the following topics should still be considered.

Executive Summary

The executive summary should provide a snapshot of the project and its privacy impacts. It should briefly summarize the PIA, including an introduction to the project, the identification of the timeline/scope, the provision of additional relevant points and a list of the risks and mitigation activities identified through the PIA.

The summary should briefly describe the kinds of information involved in the project; while the PIA should describe individual information fields involved, the executive summary should discuss the types or categories of information involved. For example, while the executive summary may indicate that demographic information is collected, the PIA contents should list the individual fields involved within the overall category of demographic information.

OIPC Expectations

Enough detail should be included in the Executive Summary that a reader would quickly understand the project, the information involved, affiliated privacy risks and suggested mitigation activities.

Introduction

The introduction should include information about the public body and the project; there should also be a discussion of the objectives of the project and how this contributes to the mandate of the public body. The description should include high level details of the impact the project will have on the current process or system. Public bodies experiencing difficulty in describing this should refer to Appendix C – Project Impact.

The introduction should also provide details of the PIA, such as when the PIA was written, the scope of the assessment, the methodology used (interviews, literature review, etc.), and the sources of information.

OIPC Expectations

After reading the introduction, the OIPC expects to have a clear understanding of the project and the scope of the PIA.

Project Description

The project description will provide additional details regarding the project. This section may include subsections on:

- Information Fields / Inventory of Personal Information
- Collection, Use and Disclosure
- Data Flows/ Personal Information Flows
- User Accounts / Access Controls
- Lifecycle

Information Fields/Inventory of Personal Information

In order to assess the impact a project will have on privacy, it is important to document what personal information is involved. A PIA should document all information that is collected, used and disclosed. For example, while the executive summary may indicate that demographic information is collected, this section should list all the individual information fields collected. The authorities for the collection should be provided; in many instances it will be section 61(c) of the *ATIPPA, 2015*. Public bodies should provide details of how the information relates to and is necessary for an operating program or activity of the public body.

In addition to the information fields being collected, details surrounding the collection should be provided. For example, is the information being collected directly or indirectly, who collects the information and how is notice provided to individuals? What happens to the information once it is collected? If it is used, who uses it and what are acceptable uses? If it is disclosed, to whom is it disclosed, how is it disclosed and what are the acceptable uses of the information once it is disclosed?

If the PIA indicates that personal information is going to be de-identified or anonymized, definitions should be provided for these terms; as well, the process that will make this happen should be described.

For additional information on personal information as defined by the *ATIPPA, 2015*, see Appendix D – Personal Information.

For additional details on collection, use and disclosure under the *ATIPPA, 2015*, please see the questionnaire in Appendix E – Collection, Use and Disclosure Questionnaire.

Data Flows/Personal Information Flows

A public body is required to protect personal information in its custody or under its control by putting reasonable safeguards in place to protect against such risks as unauthorized access, collection, use, disclosure or destruction. In order to better ensure appropriate safeguards are in place, public bodies should ensure that the safeguards, data flows and business processes are documented and understood. It is difficult to ensure appropriate safeguards are in place if it is not known what information is involved, why it was collected, where it is located, and how users access the information.

If the PIA involves an electronic system, this section should be completed collaboratively with members of the security and/or technical architecture team. Some PIAs may include both data architecture diagrams and data flow diagrams, depending on the complexity and size of the project.

For more information, please see Appendix F – Data Flows/Personal Information Flows.

User Accounts/Access Controls

Data flows are closely tied to access controls. It is important to document who has access, what they are able to do with their access (permissions) and how they access the system. Many organizations use role-based access control (RBAC), which establishes standard levels of access for specific roles or job functions. Some of the permissions that may be affiliated with various roles include:

• Create • Read • Write • System Configuration • Add/Delete Accounts • Copy Information (electronic and/or print)	• Delete • Assign • Correct/update • Remove Information (take chunks and place on portable media, etc) • Communications (manage all users emails and messages)

It should also detail any application process that must be completed, discuss acceptable use, outline the system specific training and discuss the audit capabilities of the system.

One role that is important to document is IT support models, especially when support is provided by a third party. Many electronic systems provide extensive access to those providing technical

support and generally mitigation efforts are undertaken, such as frequent audits and additional training on acceptable uses.

Some of the necessary information may already be documented in a Threat Risk Assessment (TRA), which focuses on the confidentiality, integrity and availability of the system and will usually establish priority areas for support. The Privacy Subject Matter Expert (SME) writing the PIA may decide to critically review the TRA from a privacy impact point-of-view and incorporate a summary of pertinent content in the PIA. If a public body does not discuss safeguards and merely indicates that a TRA has been completed, the OIPC would expect a copy of the TRA to be included with the PIA. The OIPC would prefer a robust description of the safeguards in place and/or a summary of pertinent TRA content.

Lifecycle

The lifecycle of information tracks information from collection to destruction. It is important to document how long information is retained and provide details of acceptable destruction.

OIPC Expectations

The project description section of the PIA is quite comprehensive. Readers should understand the project, as well as the information collected, all data flows and access details. In general, the OIPC would expect:

- Details regarding the information collected, including the information fields collected, how it is collected (source of the information), why it is required for the identified purpose, how accuracy is addressed and how individuals are notified of the collection:
    - Public bodies may attach a collection notice or form to its PIA if one was used in the collection of personal information
    - Public bodies should provide details of any legislative authorities or agreements authorizing the collection
- Discussion of how the information is used and disclosed, as well as how it is stored, transferred and securely disposed
- Details of end user training and policies and procedures; while general privacy training and policies and procedures may be discussed, the OIPC is most interested in project specific training and policies and procedures
    - This documentation should include details and examples of acceptable uses for all users, including those providing support and acting as system administration
- Information flow diagram and discussion, including safeguards
- Details of audit program and overall system capabilities for auditing
- Details regarding access, including the access levels and the process for gaining access for all users, including system administrators and third party support
- Discussion of any safeguards contained in contracts and/or agreements with third parties developing the system, providing support and/or hosting the system

Risk Assessment

A PIA is a process meant to assess the impact a project will have on the privacy of individuals; it is a critical analysis. All projects involve risk and an important part of the PIA process is the identification of risks to personal information and the suggestion of corresponding mitigation strategies. Common risks include the requirement to develop written policies and procedures for the project, the development of consent forms and privacy notices, and breach detection.

See Appendix G – Risk Assessment Methodology for additional details on risk assessment.

OIPC Expectations

The OIPC would expect to see risks identified and acknowledged, with suggested mitigation activities for each. The PIA should also provide details on the public bodies risk methodology and the overall process that is followed once risks are identified. For example, is there a project risk log that reflects the risks identified by all Subject Matter Experts on the project team?

Project Benefits

The PIA should also include a discussion of the benefits of the project. This is especially important if the PIA reveals a number of high risks areas, as it should also document how the benefits of the project outweigh any negative impact the project will have on privacy.

OIPC Expectations

The OIPC will be relying on the same test the Privacy Commissioner of Canada utilizes, which is based on the four part test of *R. v. Oakes:*

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy-invasive way of achieving the same end?

Privacy Analysis

While some PIA templates incorporate a discussion of the fair information principles throughout the PIA, others have a section that addresses the 10 principles. Somewhere in the PIA, the following should be discussed:

- Accountability
    - Identify an individual responsible for privacy and ensuring compliance with the ATIPPA, 2015 for this specific project
    - Develop project specific policies and procedures to better ensure compliance
- Identifying Purpose
    - Document the purpose of the project; all collection, use and disclosure of information should be tied back to this purpose

  - Identify the reason why the project requires the information being collected
  - Develop a privacy notice for the project; this notice should state the reason for the collection and highlight information handling processes
- Consent
  - Determine how informed consent will be implemented
  - Determine if express consent is required or if implied consent is acceptable
- Limiting Collection
  - Review each information field collected and ensure all are required for the identified purpose
  - Train front line staff so they are able to discuss why the information is required and are aware of the appropriate contact should the individual have additional questions
- Limiting Use, Disclosure and Retention
  - Document acceptable uses and disclosures, as well as retention periods and the destruction process
  - Ensure information used to make a decision about the individual is retained for a reasonable length of time (minimum of one year is prescribed in section 65 of the ATIPPA, 2015)
- Accuracy
  - Ensure that the information collected is as accurate and as up-to-date as necessary for the identified purpose
- Safeguards
  - Document how information is protected against loss, theft, unauthorized access, disclosure, copying, use or modification; safeguards should be in place for all formats, including paper and electronic records
  - Describe the auditing capabilities of electronic systems and discuss any auditing program affiliated with the project
- Openness
  - Develop and make readily available project specific information handling policies and procedures
- Individual Access
  - Document how individuals are able to obtain information about themselves, including details of how the information is used and any disclosures that have occurred
  - Develop a process for handling any requests to correct or amend information
  - Develop a process for handling access requests related to the project
- Challenging Compliance
  - Develop a process for handling complaints regarding access and privacy, including the investigation process

OIPC Expectations

The OIPC expects to see all 10 privacy principles addressed in the PIA. While some PIAs will devote a section to this discussion, others will weave the discussion throughout the document. No matter the template, the OIPC expects to see all these points discussed and documented in the PIA.

Conclusion

The conclusion of a PIA should reiterate key points from the document and discuss any action items at a high level; it should also address future plans regarding risks, risk mitigation and PIA review. The conclusion of a PPIA should also contain a recommendation for a full PIA report or provide the reasons why it has been concluded that a full PIA report is not required.

OIPC Expectations

The OIPC expects to see a discussion of how the contents of the PIA will be incorporated into the project plan moving forward. When will the PIA be reviewed again? And who is responsible for addressing the impacts and mitigation activities recommended within?

In addition, in the case of a PPIA, the OIPC would also expect to find a detailed discussion of why a PIA report has not been recommended.

Where should I begin?

While a privacy subject matter expert (SME) is generally the lead on the PIA, they rely on the project manager and others who can provide expertise. To start the process, the privacy expert may seek the following information from the project manager:

- What personal information do we collect and is it sensitive?
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?
- Who has access to or uses it?
- To whom is it disclosed?
- When is it disposed of?

The privacy SME may have to add additional information and follow-up, but this is a place to start.

PIA Resources

The OIPC would like to recognize the many great resources produced by other jurisdictions; many of these documents were leveraged in the development of this document. In particular, the OIPC NL would like to recognize:

- Office of the Information and Privacy Commissioner of Alberta
  - PIA Requirements
- Office of the Information and Privacy Commissioner of Ontario
  - Planning for Success: Privacy Impact Assessment Guide
- Office of the Information and Privacy Commissioner of British Columbia
  - Early Notice and PIA Process
- Privacy Commissioner of Canada
  - PIA Resources and Fair Information Principles
- Manitoba Ombudsman
  - PIA Tool

Appendix A – Sample Table of Contents

This sample Table of Contents is provided for assistance. As long as the key ingredients are present, as described throughout this document, a PIA can be organized and presented in a way which best suits the public body.

Executive Summary

Summarize the PIA; provide enough details so that the project and privacy impacts are understood. Include a list of all risks identified through PIA, including the risk level and suggested mitigation activities.

Introduction

Include information about your organization, the project, and the PIA.

Project Description

The project description section of the PIA is quite comprehensive and should provide details of all aspects of the project. Subheadings for this section could include:

- Project benefit
    - Critical analysis of how benefits outweigh privacy impacts of project
- Information fields / inventory of personal information
- Collection, use and disclosure
    - Provide details of collections, uses and disclosures, including authority for each
    - Clearly define acceptable uses of the information
    - List all sources of information
- Data Flows / Personal Information Flows
- Data architecture diagrams
- Known Safeguards
    - Audit capabilities and programs
    - User accounts / access controls
        - User roles
        - Details of how users will register
        - Training for end users
        - Support tiers
- Lifecycle
- Existing risk documentation

Privacy Analysis

Conduct an analysis based on the principles of the Canadian Standards Association Model Code for the Protection of Personal Information. This analysis should address each of the principles; this section should also incorporate any specific piece of legislation or other codes that apply to the project. The 10 principles are:

- Accountability
- Identifying Purpose
- Consent
- Limiting Collection

- Limiting Use, Disclosure and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Risk Assessment and Recommendations

Introduce the organization's risk methodology and risk management process. Identify the risks, evaluate the risk level for each risk and suggest mitigation activities where possible.

Conclusion

The conclusion of a PIA should reiterate key points from the document and discuss any action items at a high level.

If this template is being used for a PPIA, the conclusion should also contain a recommendation for a full PIA report or provide the reasons why it has been concluded that a full PIA report is not required.

Appendix B - Summary of OIPC Expectations

General Expectations Regarding PPIA/PIAs

- The OIPC expects public bodies to be aware of their obligations under the *ATIPPA, 2015*, as well as the authority and mandate of the Commissioner under the *ATIPPA, 2015*.

- Public bodies should be aware of what a PIA is, when a PIA should be conducted, the resources available and the benefits of conducting a PIA. Any PIA sent to the OIPC for review, either as part of the PIA review process or other investigation, should be understandable. If the PIA references a document, the document should either be summarized or attached as an appendix; if the document is publicly available, a link to the document is sufficient.

- Any project that collects, uses or discloses personal information should have documentation assessing the impact the project has on an individual's privacy. Such documentation may be in a PPIA, PIA, risk assessment, etc.

- While some organizations believe that PPIAs and PIAs need only be done on new or re-designed projects, it is best practice to complete PIAs on all projects, including current projects. All public bodies need to comply with the *ATIPPA, 2015* and a PIA is one tool that is helpful in ensuring compliance.

- The OIPC would expect public bodies to document when a PIA should be considered and, if preliminary assessments are conducted, the analysis and documentation required if it is determined a full PIA report is not required.

OIPC Expectations Organized by Section:

Executive Summary

Enough detail should be included in the Executive Summary that a reader would quickly understand the project, the information involved, affiliated privacy risks and suggested mitigation activities.

Introduction

After reading the introduction, the OIPC expects to have a clear understanding of the project and the scope of the PIA.

Project Description

The project description section of the PIA is quite comprehensive. Readers should understand the project, as well as the information collected, all data flows and access details. In general, the OIPC would expect:

- Details regarding the information collected, including the data fields collected, how it is collected (source of the information), why it is required for the identified purpose, how accuracy is addressed and how individuals are notified of the collection:
    - Public bodies may attach a collection notice or form to its PIA if one was used in the collection of personal information
    - Public bodies should provide details of any legislative authorities or agreements authorizing the collection

- Discussion of how the information is used and disclosed, as well as how it is stored, transferred and securely disposed.
- Details of end user training and policies and procedures; while general privacy training and policies and procedures may be discussed, the OIPC is most interested in project specific training and policies and procedures.
    - This documentation should include details and examples of acceptable uses for all users, including those providing support and acting as system administration
- Information flow diagram and discussion, including safeguards
- Details of audit program and overall system capabilities for auditing
- Details regarding access, including the access levels and the process for gaining access for all users, including system administrators and third party support
- Discussion of any safeguards contained in contracts and/or agreements with third parties developing the system, providing support and/or hosting the system

Risk Assessment

The OIPC would expect to see risks identified and acknowledged, with suggested mitigation activities for each. The PIA should also provide details on the public bodies risk methodology and the overall process that is followed once risks are identified. For example, is there a project risk log that reflects the risks identified by all Subject Matter Experts on the project team?

Project Benefits

The OIPC will be relying on the same test the Privacy Commissioner of Canada utilizes, which is based on the four part test of *R. v. Oakes:*

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy-invasive way of achieving the same end?

Privacy Analysis

The OIPC expects to see all 10 privacy principles addressed in the PIA. While some PIAs will devote a section to this discussion, others will weave the discussion throughout the document. No matter the template, the OIPC expects to see all these points discussed and documented in the PIA.

Conclusion

The OIPC expects to see a discussion of how the contents of the PIA will be incorporated into the project plan moving forward. When will the PIA be reviewed again? And who is responsible for addressing the impacts and mitigation activities recommended within?

In addition, in the case of a PPIA, the OIPC would also expect to find a detailed discussion of why a PIA report has not been recommended.

Appendix C - Project Impact

The following considerations have been derived from the OIPC Ontario's document "Planning for Success: Privacy Impact Assessment Guide", available online at:

https://www.ipc.on.ca/images/Resources/Planning%20for%20Success%20-%20PIA%20Guide.pdf

These considerations may assist public bodies when discussing the impact of a project. Please note that these are considerations and this does not represent a comprehensive list of project characteristics.

Consider the key characteristics of the project. Does it:

- Involve creating a new program, process, service, technology, information system or other type of IT application
- Involve a change to an existing program, process, service, technology, information system or other type of IT application
- Involve procuring goods or services
- Involve outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or destruction of personal information
- Involve developing a request for bids, proposals or services
- Involve a process, system or technology for which the privacy risks are not known or well documented
- Involve creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases
- Involve information sharing (internal and external)
- Involve the need to identify, authenticate or authorize users – public and/or internal staff
- Other activities that may impact privacy

Also consider the changes that will result from the project. Does it:

- Involve a change in business owner
- Involve a change to legislative authority
- Involve a change in users (internal and external) of a related process or system
- Involve a change in partners or service providers (internal and external)
- Involve a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of
- Involve a change to the purposes for which personal information will be collected, used or disclosed
- Involve a change from direct to indirect collection of personal information
- Involve a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information
- Involve a change to, or elimination of, existing practices of anonymizing or de-identifying information

- Involve a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software
- Involve a change to an information system or database containing personal information
- Involve a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records, or the creation of a new website to provide services to clients
- Involve a change in security requirements or measures

Appendix D – Personal Information

Some public bodies may require assistance in understanding what is considered personal information. Personal information is defined in section 2(u) of the *ATIPPA, 2015*:

> *(u) "personal information" means recorded information about an identifiable individual, including*
>
> *(i) the individual's name, address or telephone number,*
> *(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,*
> *(iii) the individual's age, sex, sexual orientation, marital status or family status,*
> *(iv) an identifying number, symbol or other particular assigned to the individual,*
> *(v) the individual's fingerprints, blood type or inheritable characteristics,*
> *(vi) information about the individual's health care status or history, including a physical or mental disability,*
> *(vii) information about the individual's educational, financial, criminal or employment status or history,*
> *(viii) the opinions of a person about the individual, and*
> *(ix) the individual's personal views or opinions, except where they are about someone else;*

To assist public bodies in developing an inventory of personal information, the following table includes types of categories of personal information and examples of information that may be collected under each category. Please note that this list of personal information is not exhaustive. A public body may have other types of personal information in its custody and or under its control, or additional information that may be considered personal information due to context. There must be a reasonable expectation that an individual can be identified from the information (either alone or when combined with other information) for the information to qualify as personal information.

Type or Category of Personal Information	Examples of Type/Category Descriptions (please note descriptions are for assistance purposes and should only be considered examples, not an exhaustive list of sub categories)
Name	First Last Middle
Address	Street Address Mailing Address City Postal Code Province

Telephone Number	Area Code Home Number Cell Number Business number
Race, national or ethnic origin, colour, or religious or political beliefs or associations	Legal entitlement to work in Canada Religion Place of Birth Membership in or support for political parties
Age	Date of Birth Year of Birth Age at Time of Collection
Sex	
sexual orientation	
marital status or family status	Single Married Divorced Co-Habitation/Common Law Widowed
identifying number, symbol or other particular assigned to the individual	MCP Driver's License Social Insurance Number Employee Number Other
fingerprints	
blood type	
inheritable characteristics	Genetic information
information about the individual's health care status or history, including a physical or mental disability	Self-identification as an individual who, for the purposes of employment, consider them to be disadvantaged due to a long term or recurring disability Medicals for employment purposes

	WHSCC Information Pregnancy status
information about the individual's educational status or history	Highest level of education received Grades Academic Achievements Disciplinary action (Suspensions, expulsions, etc.)
information about the individual's financial status or history	Bankruptcies Direct deposit information Wage garnishments Deductions from cheques Collection agency information
information about the individual's criminal status or history	Vulnerable sector check Certificates of Conduct Direct questioning if they have been convicted of a crime; if they are legally entitled to operate a vehicle, etc.
information about the individual's employment status or history	Resume information Disciplinary actions, such as suspensions and terminations Complaint information, such as Labour Relation Board Decisions WHSCC Details Specific payroll deduction details, such as wage garnishments, health insurance coverage, etc. Leave status (long term disability, parental leave, sick leave, etc).
the opinions of a person about the individual	
the individual's personal views or opinions, except where they are about someone else	

Please provide details of any additional information that is collected. When listing all collected information, consider if non-personal information could be combined or linked to enable the identification of an individual.

Appendix E – Collection, Use and Disclosure Questionnaire

In June 2015, Service Alberta published two new PIA templates to assist privacy subject matter experts in assessing and ensuring privacy compliance is met. The following questionnaire leverages Alberta's template and has been customized to this province's *ATIPPA, 2015*. It is meant to assist public bodies that are unsure of their legislative authority to collect, use and disclose information. Public bodies interested in the Alberta questionnaire can see both templates at http://www.servicealberta.gov.ab.ca/foip/.

The *Protection of Privacy Policy and Procedures Manual* developed by the Access to Information and Protection and Privacy (ATIPP) Office is a good resource for any public body seeking additional information on collection, use and disclosures in general, as well as specific details of the *ATIPPA, 2015.*

Part 1

- Does the program collect, use or disclose personal information as defined in section 2(u) of the *ATIPPA, 2015*?
    - While not a comprehensive list, the following areas commonly collect, use and disclose personal information: customer service, complaints, human resources, finance/ purchasing, information technology, security, legal services.
- TIP: business versus personal information. Information that may seem personal, such as name and contact information, may not represent an unreasonable invasion if that personal information relates to an individual's business activities, that is, they are acting in a professional capacity in the context of the information. When determining if the program involves personal information, consider the context of the information.

Part 2: Collection (Section 61)

Is this program collecting personal information? **Yes** ☐ **No** ☐

If the answer is yes, continue under this part of the assessment.
If the answer is no, go to Use under Part 5 of this assessment.

There are three authorities for a public body to collect personal information under the ATIPPA, 2015. Please think about all personal information data elements collected. The collection of some personal information data elements may have a different authority than other personal information data elements and we must identify every authority that applies. Check all that apply.

☐ The collection of the personal information is expressly authorized by an enactment of Newfoundland and Labrador or Canada. (section 61(a))

If yes, provide the legislative authority, including the name and section of Act.

☐ The collection of the personal information is for law enforcement (section 61(b))

NOTE: *law enforcement is defined under section 2(n) of the ATIPPA, 2015. In order to apply this authority, please review this definition and indicate whether 2(n)(i) or 2(n)(ii) applies.*

☐ The collection of personal information is directly related to and necessary for an operating program or activity of the public body under this program. (section 61(c))

NOTE: *if a public body intends to proceed on the basis that the collection is "necessary", it should be prepared to explain why the collection is necessary.*

If you have checked any of these three authorities above for collection, you have identified an authority under the *ATIPPA, 2015* that allows the program to collect the personal information. Please continue the assessment.
If the answer is no to all three of these authorities listed above, you have not identified an authority under the *ATIPPA, 2015* that allows the program to collect the personal information. Please contact the ATIPP Office or your ATIPP Coordinator for assistance.

Part 3: Direct/Indirect Collection (section 62)

Personal information must be collected directly from the individual unless an exception to this requirement applies.

Is the program only collecting personal information directly from the individual the information is about? **Yes** ☐ **No** ☐

If the answer is yes, go to Notification under Part 4 of this Assessment.
If the answer is no, and you are planning to collect any personal information indirectly, continue under this part of the assessment.

Please indicate whether any of the following statements are true.

☐ The individual authorized (consented to) another method of collection.(section 62(1)(a)(i))

- *If yes, please explain how the authorization is obtained.*

☐ Another Act or regulation authorizes the indirect collection (section 62(1)(a)(iii).

- *If yes, please provide the legislative authority, including the name of the Act and the applicable section.*

☐ The Information and Privacy Commissioner has authorized the indirect collection (section 62(1)(a)(ii) with section 95(1)(c)).

- *If yes, please provide any details in relation to the Commissioner's authorization, such as expiry, conditions, etc.*

☐ The information may be disclosed to the public body under the *ATIPPA, 2015* (sections 68-71);
- *If yes, please provide the section of the ATIPPA, 2015 under which the personal information is disclosed to the public body*

☐ The indirect collection is for the purpose of determining suitability for an honour or award (section 62(1)(c)(i));

☐ The indirect collection is for the purpose of an existing or anticipated proceeding before a court or a quasi-judicial tribunal (section 62(1)(c)(ii);

☐ The indirect collection is for the purpose of collecting a debt or fine or for making a payment (section 62(1)(c)(iii));

☐ The indirect collection is for the purpose of law enforcement (section 62 (1)(c)(iv));

NOTE: Law enforcement is defined under section 2(n) of the ATIPPA, 2015. In order to apply this authority, please review this definition.

☐ The indirect collection is in the interest of the individual and time or circumstances do not permit direct collection (section 62(1)(d))

If you have checked one of the preceding authorities for indirect collection, you have identified an authority under the *ATIPPA, 2015* to collect the personal information from another source rather than directly from the individual(s) themselves. Notification is not required: skip to Use under Part 5 of this assessment.
If none of these indirect collection authorities is selected, you must collect the personal information directly from the individual the information is about or identify options that meet one or more of these authorities. Please contact the ATIPP Office for assistance.

Part 4: Notification (section 62(2))

Notification is required when personal information is collected directly from an individual. This part of the assessment is completed when you are collecting information directly from individuals. Notifications contain <u>three</u> elements:

1) Purpose of collection – this must be specific enough so a reasonable person can understand the purpose for which their personal information is collected including how it may be used and/or disclosed.

2) Specific legal authority for collection – this should include any enabling legislation and/or applicable *ATIPPA, 2015* authority.

3) Job title, business address and business telephone number of an officer or employee of the public body who can answer questions about the collection.

Does the notification provided to the individual at the time personal information is collected under this program include the three elements listed above? Yes ☐ No ☐

Briefly describe how notification for the direct collection of personal information is provided under this program:

_____

_____

_____

Please note that, if the exemptions listed in section 62(3) apply, notification is not required. If a public body determines that these exemptions apply, please provide the exemption being used and details regarding its application.

Part 5: Use (section 66)

Is the program using personal information? **Yes** ☐ **No** ☐

If the answer is yes, continue under this part of the assessment.
If the answer is no, go to disclosure beginning at Part 6 of this assessment.

There are three use authorities for personal information under the ATIPPA, 2015. Please think about all personal information data elements involved; the use of some personal information data elements may have different authority than other personal information data elements. Check all that apply.

☐ The personal information is being used under this program according to the original purpose for which it was collected or compiled or for a use that is consistent with that original purpose of collection (section 66(1)(a)).

If the above is selected and the use includes consistent purpose, please confirm the consistent use meets both of the following:

☐ The consistent use has a reasonable and direct connection to the purpose for which the personal information was originally collected or compiled.

AND

☐ The consistent use is necessary for performing the statutory duties of or operating a legally authorized program of the public body using the personal information.

Provide details/explanation: _____

_____

☐ The individual has identified the information and consented to the use (section 66(1)(b))
Consent has specific requirements for validity whether in writing or verbally. Please review the elements of consent in the Protection of Privacy Policy and Procedures Manual and/or discuss the requirements for valid consent with the ATIPP Office.

☐ The use is for a purpose for which the information was disclosed to the public body under sections 68 to 71 (section 66(1)(c))

If the information is being disclosed by a public body under the authority of sections 68 to 71 of the ATIPPA, 2015, this is the corresponding authority for the public body receiving the information to use it.

If this program receives and uses personal information disclosed from another public body and you are uncertain if it is being disclosed under the ATIPPA, 2015, you may wish to return to this question after reviewing the authorities in Disclosure beginning at Part 8 of this assessment and in consultation with the other public body.

☐ If you are a post-secondary educational body, section 67 authorizes the use of personal information in alumni records for the purpose of its own fundraising activities, where that personal information is reasonably necessary for the fundraising activities. Section 67 establishes criteria that must be met to ensure compliance with the *ATIPPA, 2015*.

- *If you are a post-secondary educational body using information under the authority of section 67, please describe/explain how you are in compliance with the requirements established in section 67(2), 67(3) and 67(4).*

If you have checked one of the preceding authorities for use, you have identified an authority under the *ATIPPA, 2015* that allows the program to use the personal information. Please continue the assessment.
If none of these use authorities is selected, you have not identified an authority under the *ATIPPA, 2015* that allows the program to use the personal information. Please contact the ATIPP Office for assistance.

Part 6: Disclosure for Research or Statistical Purposes (section 70)

Has a researcher requested records that contain personal information as part of this program?

Yes ☐ No ☐

If the answer is yes, then all the conditions under section 70 of the *ATIPPA, 2015* must be met including signing an agreement to comply with the approved conditions. Please contact the ATIPP Office for assistance.
If the answer is yes, and this is the only disclosure, go to Accuracy and Retention under Part 9 of this assessment.
If the answer is yes, and there may be additional disclosure authorities, or if the answer is no, go to Disclosure for Archival or Historical Purposes under Part 7 of this assessment.

Part 7: Disclosure for Archival or Historical Purposes (section 71)

The Provincial Archives of Newfoundland and Labrador and the archives of a public body may disclose personal information as authorized by section 71 of the ATIPPA, 2015.

Is the disclosure of personal or other information held in an archives part of this program? Yes/No

If the answer is yes, and this is the only disclosure, go to Accuracy and Retention under Part 9 of this assessment.
If the answer is no, go to Disclosure of Personal Information under Part 8 of this assessment.

Part 8: Disclosure of Personal Information (section 68)

Is the program disclosing personal information? Yes ☐ No ☐

If the answer is yes, continue under this part of the assessment.
If the answer is no, go to accuracy and retention under part 9 of this assessment.

There are many authorities that allow for a public body to disclose personal information under the ATIPPA, 2015. Please think about all personal information data elements disclosed and all instances of disclosure; the disclosure of some personal information data elements may have a different authority than other personal information data elements. Additionally, a disclosure to one public body or organization may have a different authority than a disclosure to another one.

Under section 68(2), a public body may disclose personal information only to the extent necessary to enable the public body to carry out the purpose for disclosure (described in the disclosure provisions that follow) in a reasonable manner.

Check only those types of disclosure that are specifically intended to occur under the program under assessment.

☐ The disclosure is in accordance with an *ATIPPA, 2015* access request (section 68(1)(a));

☐ The individual has identified the information and consented to the disclosure in the manner set by the Minister responsible for the Act (section 68(1)(b)).

Consent has specific requirements for validity whether in writing or verbally. Please discuss the requirements for valid consent with the ATIPP Office.

☐ The personal information is being disclosed under this program according to the original purpose for which it was collected or compiled or for a use that is consistent with that original purpose of collection (section 68(1)(c)).

If the above is selected and the use includes consistent purposes, please confirm the consistent use meets both of the following:

☐ The consistent use has a reasonable and direct connection to the purpose for which the personal information was originally collected or compiled.

AND

☐ The consistent use is necessary for performing the statutory duties of or operating a legally authorized program of the public body using the personal information.

Provide details/explanation:

☐ The disclosure is done in order to comply with an enactment of Newfoundland and Labrador or Canada, or with a treaty, arrangement or agreement made under an enactment of Newfoundland and Labrador or Canada (section 68(1)(d)).

☐ The disclosure is to comply with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information (section 68(1)(e)).

☐ The disclosure is to an officer or employee of the public body or to a minister and is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister (section 68(1)(f)).

☐ The disclosure is to the Attorney General for use in civil proceedings involving the government (section 68(1)(g)).

☐ The disclosure is for the purpose of enforcing a legal right that the Government of Newfoundland and Labrador or a public body has against any person (section 68(1)(h)).

☐ The disclosure is for the purpose of:

i) Collecting a fine or debt owing by the individual the information is about to the Government of Newfoundland and Labrador or to a public body OR
ii) Making a payment owing by the Government of Newfoundland and Labrador or by a public body to the individual the information is about (section 68(1)(i))

- ☐ The disclosure is to the Auditor General or any other person or body prescribed in the *ATIPPA, 2015* regulations for audit purposes (section 68(1)(j)).
- ☐ The disclosure is to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem (section 68(1)(k)).
- ☐ The disclosure is to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry (section 68(1)(l)).
- ☐ The disclosure is to the Provincial Archives of Newfoundland and Labrador or to the archives of a public body for archival purposes (section 68(1)(m)).
- ☐ The disclosure is to a public body or a law enforcement agency in Canada to assist in an investigation:
  - i) Undertaken with a view to a law enforcement proceeding OR
  - ii) From which a law enforcement proceeding is likely to result (section 68(1)(n))
- ☐ Where the public body is a law enforcement agency and the information is disclosed:
  - i) to another law enforcement agency in Canada OR
  - ii) to a law enforcement agency in another country under an arrangement, written agreement, treaty or legislative authority (section 68(1)(o)).

NOTE: *law enforcement is defined under section 2(n) of the ATIPPA, 2015. In order to apply this authority, please review this definition.*

- ☐ Where the head of a public body determines that compelling circumstances exist that affect a person's health or safety and where notice of the disclosure is given in the form appropriate in the circumstances (section 68(1)(p)).
- ☐ The disclosure facilitates contact with the next of kin or a friend of an injured, ill or deceased individual (section 68(1)(q)).
- ☐ The disclosure is for any purpose where an enactment of Newfoundland and Labrador or Canada authorizes or requires the disclosure (section 68(1)(r)).
- ☐ The disclosure is in accordance with section 70 (disclosure for research or statistical purposes) or 71 (disclosure for archival or historical purposes) (section 68(1)(s)).

If yes, see also Disclosure for Research or Statistical purposes and/or Disclosure for Archival or Historical Purposes under Parts 6 and 7 of this assessment.

- ☐ The disclosure is not an unreasonable invasion of a third party's privacy under section 40 (section 68(1)(t)).

NOTE: *section 40(2) lists when a disclosure is not an unreasonable invasion of privacy under formal access. If disclosure under this program is listed in section 40(2), then this disclosure provision may apply.*

- ☐ The disclosure is to an officer or employee of the public body or to a minister, if the disclosure is necessary for the delivery of a common or integrated program or service and the performance of the duties of the officer or employee or minister to whom the information is disclosed (section 68(1)(u)).
- ☐ The disclosure is to the surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy (section 68(1)(v)).

If you checked at least one of the preceding authorities for disclosure, you have identified an authority under the *ATIPPA, 2015* that allows that program to disclose the personal information. Please continue the assessment.

If the answer is not to all of these disclosure authorities above, you have not identified an authority under the *ATIPPA, 2015* that allows the program to disclose the personal information. Please contact the ATIPP Office for assistance.

Appendix F - Data Flows/Personal Information Flows

It is important to map the flow of personal information in all formats, from collection until the final destruction, as part of the privacy analysis of the initiative. Many data flows are documented in diagrams with accompanying descriptions that provide additional details on each movement. Data flow diagrams in general represent the external devices sending and receiving data, processes that change that data, data flows themselves and data storage locations. Data flows not only track the movement of the data, but also highlight any dependencies and assist in identifying critical system components. For example, if system A is compromised, it is important to note that system B also shares server space and may be impacted as well. The quicker these details are known, the quicker mitigation activities can commence.

In general, data flow diagrams and accompanying explanations should document and provide details on:

- how information is collected
- where information is stored
- what security measures are used to protect the information throughout the process
- how information may be accessed and by whom
- the circumstances surrounding any disclosure(s) of personal information, such as data protection provisions in contracts with third parties

In addition to a data flow diagram, an information flow table or diagram can help you visualize personal information flows associated with the project. As discussed in the OIPC Ontario's *Planning for Success: Privacy Impact Assessment Guide*, descriptive information flow tables may be organized by some, or all, of the following categories:

• Personal information • Source of information • Collected by • Collection method • Purpose of collection • Format of the information • Purpose of use • Used by	• Security control during information transfer • Information repository format • Storage retention site • Purpose of disclosure • Disclosed to • Retention policy • Disposal or destruction policy

For example:

Personal information	Collected By? From? How? When? Where? Why? Authority?	Used By? How? When? Where? Why? Authority?	Retained By? How? How long? Where? Why?	Secured By? How? When? Where? Why?	Disclosed By? To? How? When? Where? Why? Authority?	Disposed of By? How? When? Where? Why? Authority?

Appendix G – Risk Assessment Methodology

The OIPC NL's Risk Assessment methodology rates both the **likelihood** (probability) of an adverse event, and the **impact** (magnitude or severity of harm) of that event, on a scale of one to five. It leverages risk assessment methodology developed by the Privacy and Legislation Branch of British Columbia's Office of the Chief Information Officer.

Likelihood of Event	
Level	Descriptor
5	Almost Certain
4	Likely
3	Possible
2	Unlikely
1	Rare

Impact of Event	
Level	Descriptor
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Determining the Impact

To determine the impact of an event, public bodies should consider the personal information involved and the consequences of the potential impacts. All factors identified in the impact table can, under certain circumstances, be ranked higher or lower. For example, for many, a home mailing address could be considered low risk personal information. That same home mailing address on a database of a women's shelter could be considered high risk personal information, the disclosure of which could cause safety concerns.

Factors Affecting the Impact of a Risk	Considerations (listed in order from highest impact examples to lowest)
Sensitivity of personal information	• Identity information, financial information, biometrics, health information; • Educational information, nationality; • Postal code, low sensitivity personal opinions about low sensitivity topics, e.g. the weather.
Mosaic effect of information (can be combined with other information that is publicly available to identify individuals)	• Very small population or geographic area, very unique characteristics (e.g. small town); • Moderate population or geographic area, potentially identifying characteristics (e.g. region with low population); • Large population or geographic area, common characteristics (e.g. province of NL).
Effect on individuals or third parties	• Risk of identity theft, physical harm, hurt or humiliation, or risk to business opportunities. • Pestered by marketers, inconvenienced. • No effect or unnoticed.

Audience of unauthorized disclosures	• 101+people; • 11-100 people; • 0-10 people.
Effect on public body's credibility or reputation	• Bad press, political ramifications, public outcry; • Length of time, if any, system is unavailable; • Internal ramifications, major process overhauls; • Expected, of little consequence.

Determining the Likelihood

To determine likelihood, public bodies should consider the chance of something happening.

Factors affecting the likelihood of a risk materializing	Considerations (listed in order from the most likely to the least likely)
Content is public facing (i.e. comments section for a web site or a public body's Facebook page)	• No moderation or monitoring of content; • Content is monitored or moderated during business hours only; • All content is moderated before being posted.
Group access to content	• Open access; • Role-based access to all client files (i.e. all analysts can access any client file); • Need-to-know access to client files only (i.e. only assigned analyst can access client file).
Technical security measures	• No encryption, no password protection. • Password protection only. • All content in transit is encrypted and password protected.
Physical security measures	• Open, street access (no sign-in, no pass cards). No open storage; • No identification needed for sign-in. Unescorted access; • Restricted, escorted access only.
Policy	• No access policies, no clear-set guidelines regarding information management. No education of existing policies; • Some policies in place, but no education of these policies; • Clear-set policies regarding information management and widespread education provided on these policies.

Overall Risk Score

The overall score attributed to the risk of such an adverse event occurring is calculated as the product of the likelihood and impact ratings to produce a score and risk level. Overall risk scores should be done for each identified risk. Once risks have been identified and quantified, a decision must be made on how to manage the risk.

Overall Risk (multiply impact by likelihood to calculate)	
Level	Descriptor
20+	Extreme
11-19	High
5-10	Moderate
1-4	Low