May 2015

Audit and Compliance Program Charter

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

TABLE OF CONTENTS

1.0 BACKGROUND

The Office of the Information and Privacy Commissioner for BC ("OIPC") has established an Audit and Compliance Program to assess the extent to which public bodies and private sector organizations are protecting personal information and complying with access provisions under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA").

This document provides the framework for the Audit and Compliance Program and is designed to assist public bodies and organizations to understand the authority and function of the OIPC in conducting assessments as well as the basic steps leading up to and during an assessment.

2.0 AUDIT AND COMPLIANCE ASSESSMENTS

The OIPC's Audit and Compliance Program draws from a combination of compliance assessment; operational audit; information management and information technology audit; program evaluation; and process improvement methodologies. The purpose of the Audit and Compliance Program is to provide a mechanism to:

- enhance oversight regarding the management of personal information across BC;
- measure the level of compliance employed by public bodies and organizations with provincial privacy and access legislation, relevant policies and guidelines, and privacy principles; and
- make recommendations, where needed, to improve privacy and access practices, policies, guidelines, and legislation.

The Audit and Compliance Program will comprise fair and objective assessments of public bodies or private sector organizations to determine:

- how well entities comply with obligations under FIPPA or PIPA, relevant policies and procedures, guidelines, and privacy principles;
- whether entities maintain adequate administrative, physical and technological safeguards to protect personal information from unauthorized access, collection, use, disclosure, disposal or similar risks;
- the extent to which an entity has established and maintains adequate procedures for managing requests for information; and
- the extent to which an entity has established and maintains an effective and accountable privacy management program.

Assessments will identify both the areas where an entity may excel with regard to compliance, safeguards, and overall access or privacy management; as well as areas where improvements are needed in order to comply with legislation and guidelines.

There are many aspects within access or privacy management programs that can be assessed to determine the extent to which public bodies and private sector organizations are protecting

personal information and complying with access provisions. Some of these include, for example:

- **Management, Policies and Procedures**: Reviewing an entity's management of access to information and protection of privacy programs; access to information and privacy policies and procedures; and information and data sharing agreements.
- **Collection, Use, Disclosure and Retention**: Assessing the collection, use, disclosure and retention of personal information by the entity; whether appropriate notice and consent has been obtained; and whether the entity limits collection, use, disclosure and retention of personal information to only what they need to administer a program or business.
- **Protections and Safeguards**: Examining an entity's access, disclosure or protection provisions; their administrative, technical and physical safeguards; staff knowledge and training related to privacy and the protection of personal information; and whether and how an entity protects personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.
- **Access Processes**: Reviewing an entity's access to information processes; how it handles access-related requests or complaints; timelines for responding to access requests; and compliance with other access-related obligations under FIPPA or PIPA.
- **Accountability and Compliance Monitoring**: Evaluating how the entity monitors compliance with its privacy policies and procedures; accountability practices; how it handles privacy-related complaints; whether they conduct internal or external audits of safeguards; and whether they analyze breaches that may have occurred.

In order to objectively identify locations and topics for assessment, OIPC staff will interview stakeholders; conduct analysis of internal files (complaints, requests for review and breaches); review information collected from other entities; and consider other investigations and policy projects recently completed, currently underway or about to be initiated.

3.0 KEY LEGISLATIVE AUTHORITY AND POWERS

Public bodies or organizations being reviewed under the Audit and Compliance Program may be assessed on any aspect of their FIPPA or PIPA obligations with regard to access, collection, use, disclosure, protection, retention, or disposal of personal information. The Commissioner has the following powers with regard to such assessments:

- monitoring and compliance (FIPPA s. 42 and PIPA s. 36)
    - investigate or audit to ensure compliance with any provision of these Acts or regulations,
    - make orders resulting from investigations or audits,
    - receive comments from the public, and
    - engage in or commission research into anything affecting the achievement of the purposes of the Acts;

- compel records and answers to questions (FIPPA s. 44 and PIPA s. 38);
- entry and inspection (PIPA s. 38);
- inform the public about the Acts or make comment (FIPPA s. 42 and PIPA s. 36); and
- delegate her duties, powers and functions to any person (FIPPA s. 49 and PIPA s. 43)

Assessments may comprise investigation, audit, research or any combination of the monitoring and compliance functions.

There are also several sections in both FIPPA and PIPA that provide certain protections to individuals who have made statements or answered questions during an assessment by the OIPC, including:

- general restriction on disclosure by Commissioner and staff (FIPPA s. 47 and PIPA s. 41)
- the Commissioner or staff cannot be compelled to give evidence in court respecting information collected while performing their duties (FIPPA s. 45 and PIPA s. 39);
- protection against libel or slander actions (FIPPA s. 46 and PIPA s. 40); and
- whistleblower protections (FIPPA s. 30.3 and PIPA s. 54).

Please see Appendix 1 for more detail regarding the legislative authority and powers of the Commissioner.

4.0 VALUES

All activities related to the planning and implementation of an assessment will be conducted in accordance with a set of values promoted by the OIPC. OIPC staff members conducting assessments will endeavour to act at all times with:

- independence;
- confidentiality;
- due care;
- integrity;
- objectivity;
- competence;
- a systematic and structured approach;
- secure handling of information; and
- appropriate supervision.

5.0 STEPS IN THE ASSESSMENT PROCESS

5.1 Step One: Planning

5.1.1 Identifying Scope and Objectives: the "What" and "Why"

The scope of an OIPC assessment will often comprise an evaluation of compliance with any aspect of FIPPA, PIPA, OIPC guidelines, entity policies, and/or safeguards for protecting personal information. The objectives may include measuring compliance; contributing to a body of knowledge on a particular topic; updating OIPC guidance documents; recommendations for amendments to policy or legislation; or other purposes.

5.1.2 Assessment Targets: the "Who"

The OIPC will select topics or entities to assess based on a variety of factors and resources, including:

- complaints received by the OIPC;
- media reports relating to privacy practices within a particular entity, sector or topic;
- follow-up with previously assessed entities;
- other assessments that point to further need to explore a similar entity, topic, geographical region;
- comments from consultation with FOI, privacy and security experts;
- information that an entity collects or uses a substantial amount of personal information, or very sensitive personal information; and/or
- a need to explore a particular topic or entity for input into policy or legislative amendments.

5.1.3 Notifying the Entity: the "When" and "Where"

The OIPC will notify involved entities in advance of an assessment. We will send a letter to the head(s) of the entity(ies) involved outlining the intention to conduct an assessment as well as a general outline of the scope, objectives, methodology and anticipated timelines.

The OIPC will also share a draft of a comprehensive Assessment Plan with entity representatives in advance. The Assessment Plan will provide high level information on:

- the reasons why an entity was selected for assessment;
- the scope, objectives and basic methodology for the assessment;
- the topics, programs, technology or initiatives that will be assessed;
- the job functions of entity staff who will be interviewed;
- background materials to be made available prior to the onsite visit;
- materials that will be reviewed throughout the course of the assessment;
- OIPC assessment team members and their role for the assessment; and
- estimated timelines for key assessment activities.

The success of any assessment depends primarily on the cooperation from entity staff; access to the systems and information needed for the assessment; and the availability of evidence for inclusion in the assessment. As such, key staff from the entity(ies) involved will be invited to comment on any challenges or issues they feel may interfere with successful completion of the assessment. In addition, advance consultation allows the assessment team to gain a better understanding of the topics intended for assessment; the types of materials available; and the structure of the entity.

5.1.4 Choosing the Methodology: the "How"

Each assessment will have unique requirements and objectives and, as such, the assessment team will select methodology for specific assessments based on the particular circumstances of the topics and entities involved. The assessment team will often use a combination of the following methodologies:

- interviews with senior entity staff;
- interviews or focus groups with key program area staff;
- inspection of the premises, with attention to programs that collect personal information and safeguards employed by the entity (for example: inspection of electronic programs or databases, reviews of security procedures, or examination of physical security measures);
- file reviews based on the nature of the business (for example, inspection of client files, access logs, communications, etc.); and
- questionnaires to assess knowledge and awareness of, satisfaction with, or attitudes toward privacy policies and processes.

5.1.5 Deliverables: Letter of Intent, Assessment Plan

As discussed above, the OIPC assessment team will draft the following deliverables during the planning phase of an assessment:

- letter of intent provided to the head of the entity; and
- the Assessment Plan.

5.2 Step Two: Background Research

5.2.1 Understanding the "Lay of the Land"

As noted above, the OIPC will provide advance notice to entities involved in an assessment. The comprehensive Assessment Plan will outline the background materials that will be requested for review prior to an onsite visit. Examples of background materials include:

- relevant written polices or procedures;
- organizational charts;
- contact information for key staff;
- descriptions of safeguards employed to protect personal information;
- copies of privacy management assessments and risk assessments conducted by the entity involved in the assessment or by other organizations;

- internal reports relating to programs under review or personal information management;
- data sharing agreements;
- privacy impact assessments;
- copies of contracts related to service providers or others who may collect, use, disclose or retain personal information on behalf of the entity involved in the assessment;
- a small sample of the types of files that may be included in a file review;
- copies of training materials and/or details regarding training programs;
- copies of communication materials regarding a program or service, and memos or directives to staff; or
- additional materials requested by the OIPC assessment team or materials that the entity involved in the assessment may identify.

The OIPC assessment team will review the background materials in order to build understanding of the context for the specific topic and entity. Most often, the team will review these materials at OIPC offices; however if materials are required to remain onsite at the entity, the team may review documents on location.

5.2.2 Building Assessment Criteria

Assessment criteria are standards against which compliance can be evaluated and assessed. The OIPC assessment team will select criteria for assessments based on appropriateness for the topic and entity for each specific assessment. Criteria are to be relevant, unbiased, fulsome, understandable and reliable. Common sources the team will use to develop assessment criteria include:

- FIPPA;
- PIPA;
- OIPC guidance documents:
    - *Accountable Privacy Management in BC's Public Sector*,
    - *Getting Accountability Right with a Privacy Management Program* (private sector),
    - *A Guide to PIPA for Businesses and Organizations*,
    - *Privacy Breaches: Tools and Resources*, and
    - Other relevant guidance documents;
- policies, standards, directives and guidelines developed by other Privacy Commissioners or relevant oversight entities;
- privacy principles:
    - Canadian Standards Association: *Model Code for the Protection of Personal Information*, and
    - Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants: *Generally Accepted Privacy Principles*;

- relevant entity policies, agreements and contract terms relating to how personal information is managed;
- standards relating to information security and information management developed by international standards bodies:
    - International Organization for Standardization ("ISO"), and
    - Information Systems Audit and Control Association ("ISACA");
- other relevant legislation, regulations, directives or enactments;
- recommendations from previous assessments or audits (internal or external);
- criteria developed by the OIPC assessment team; and
- other criteria relevant to specific assessment objectives.

Once several assessments have been completed, the OIPC will have a standard set of criteria that can be considered in future assessments. The OIPC assessment team would still review specific criteria to determine its relevance or adaptability to the particular assessment.

5.2.3 Drafting the Tools

Assessment tools are instruments on which to record the findings of any particular data collection during an assessment. The assessment team will either: (1) build these tools in advance of an assessment and review or amend them prior to the onsite visit or (2) build them after the review of background materials. The types and content of assessment tools will depend on the objectives of the specific assessment and will be developed from the assessment criteria outlined above. Examples of tools that the assessment team may use include:

- guides for use during interviews or focus groups;
- questionnaires for conducting surveys;
- inspection checklists for use during physical examination of personal information safeguards or review of electronic programs or databases; and
- spreadsheets to be used during inspection of program files.

5.2.4 Deliverables: Context Description, Assessment Tools

During the background research phase of an assessment, the assessment team will create these deliverables:

- a summary of the background of a particular program or service and the entity involved in the assessment (for inclusion in the final report);
- a description of the personal information collected and the policies and processes used to manage that information (for inclusion in the final report); and
- copies of assessment tools to be used during the fieldwork phase of the assessment.

5.3 Step Three: Fieldwork

5.3.1 Gathering Evidence: Multiple Methods

Evidence can include any information gleaned during the course of an assessment that assists evaluators in determining whether individual assessment criteria have been met. Evidence can come from interviews; physical inspections and observations; system or files reviews; or questionnaires depending on the nature of the assessment and its objectives. Evidence may also be derived from analysis of such information. In each of these methods of evidence gathering, evidence will be documented on checklists, spreadsheets, survey forms or by other means.

Most often, the OIPC assessment team will be gathering evidence by conducting one-on-one interviews with key entity or program area staff. Where possible, the team may provide in advance a basic interview guide containing some of the questions to be asked or points the interview is intending to cover. These interviews help the assessment team to gain knowledge about the entity and its relevant programs or processes, determine staff awareness and learn from staff about the topic being assessed, and collect and corroborate evidence to answer assessment questions. OIPC team members will take notes and may digitally record during the interviews in order to ensure evidence is available for later analysis and to substantiate conclusions drawn. These notes are used for the OIPC staff to review and analyze for the purposes of the assessment and will not be shared with anyone outside of the OIPC. See Appendix 1 for further information on protections for those who provide statements to the OIPC or answer questions during an assessment.

The OIPC assessment teams will seek to gather sufficient volume and completeness of evidence to be able to develop conclusions that are valid and sound enough that a reasonable person may reach the same conclusions when reviewing evidence included in the assessment. There may be occasions where the assessment team requests additional evidence (for example: additional records for review, follow-up interviews with staff to clarify points or ask additional questions, or documents that may not have been requested from the entity earlier).

5.3.2 Documenting Evidence: Substantiation Binders

The assessment team will maintain substantiation binders that detail the evidence used to support the findings documented in assessment reports. Substantiation binders may contain, for example: copies of relevant communications and background materials; initial assessment planning documents; interview or focus group notes; completed inspection or observation check-lists; and aggregate findings from questionnaires or statistical analysis.

Substantiation binders will be used for internal peer review of assessment reports in order to provide a secondary check to ensure that all findings and statements made within the report are supported by available and corroborating evidence.

5.3.3 Sharing Initial Findings: Providing Entity Feedback

The OIPC assessment will endeavour to provide entities involved in the assessment with feedback throughout the process. The assessment team will raise gaps or challenges found during the collection and initial analysis of evidence with the management or executive of the entity being assessed. Open communication and continuous feedback are beneficial in allowing entities the chance to implement quality improvement measures as soon as possible. The

ultimate goal of the OIPC Audit and Compliance Program is to improve privacy or access practices and support information rights of British Columbians.

5.3.4 Deliverable: Evidence Collected, Substantiation Binders

The OIPC assessment team will create the two key deliverables during the fieldwork phase of an assessment, including:

- documented evidence from each method used to gather evidence during the assessment; and
- substantiation binders containing key evidence.

5.4 Step Four: Analysis and Reporting

5.4.1 Analyzing Results

The OIPC assessment team will analyze the evidence collected during the fieldwork stage in order to answer the questions raised through the assessment plan (step one) and detailed by the assessment criteria (step two). Analysis may be qualitative or quantitative. Qualitative analysis is often used to explore descriptions or observations that may contain deeper meaning, for example, to determine recurring themes across interviews or focus groups. Quantitative analysis focuses on numbers and may be used, for example, to examine a bulk of questionnaires or to count the prevalence of a particular error or issue in a sample of files.

The assessment team uses both qualitative and quantitative analytical methods to interpret whether the information collected during fieldwork shows that the entity has met the assessment criteria. Analysis will reveal whether there is sufficient evidence to support an assessment finding.

5.4.2 Drafting the Report and OIPC Internal Review

The assessment team will summarize findings discovered through fieldwork and analysis, along with potential recommendations, in a preliminary report. The preliminary and all subsequent reports will usually include, at minimum:

- a description of the entity and topic being assessed;
- an outline of the objectives, scope and criteria for the assessment;
- a description of the methodology used to conduct the assessment;
- an overall assessment opinion or summary statement;
- key findings and a summary of related evidence;
- a summary of the gaps or challenges found and why these are important to address; and
- recommendations to address the gaps or challenges found.

The assessment team will share this preliminary report with other OIPC internal reviewers and the Deputy Registrar/Assistant Commissioner. The assessment team will incorporate the feedback and then submit a draft report to the Commissioner for review.

5.4.3 Entity Review and Comment

Once the draft report has been approved by the Commissioner, entities that are involved with the assessments will receive a copy of the draft report. Entities will be able to provide feedback relating to any errors, omissions or misinterpretations in the report(s). If entity reviewers have concerns regarding report findings, they can discuss them with the OIPC assessment team. The assessment team will then review the feedback and determine what changes to incorporate in the final report.

Entities will also be asked to provide an official response to the report findings and whether or not they accept the OIPC's recommendations. If entities have already implemented or initiated some of the recommendations, the assessment team will consider updating the report to include a description of the changes that have been undertaken. The team may also include the official response letter from the entity in its entirety in an appendix to the report.

5.4.4 Final Report and Public Release

The assessment team will provide the final report to the Deputy Registrar/Assistant Commissioner and the Commissioner for review and approval. Communications will be prepared for public release of the report. If instead the Commissioner decides that the report will not be made public in its entirety, then the assessment team will prepare a smaller version or an executive summary of the report for public distribution.

Prior to public release, the Commissioner will send a final copy of the full report (and, if applicable, the smaller version or executive summary for public distribution) to the entities involved in the examination.

In most cases, the Commissioner will provide a news release relating to the assessment and the final report. Media outlets may also request the Commissioner to participate in radio, print or television interviews regarding the assessment report, its findings, the recommendations, or related topics.

5.4.5 Follow-up on Recommendations

The OIPC may ask entities involved in the assessment to provide an action plan detailing how the recommendations will be implemented, along with the timelines for implementation. The OIPC assessment team will follow-up with the entities as necessary to determine the level of implementation. It is possible that a follow-up assessment will also be conducted to determine the level of compliance with the recommendations and/or to determine whether the implemented changes now meet the original assessment criteria.

5.4.6 Deliverables: Draft Report, Final Report

The assessment team will prepare the following deliverables during the analysis and reporting step of an OIPC assessment:

- documented analyses in summary documents, excel spreadsheets, highlighting or comments on interview notes;
- preliminary report and comments from internal reviewers;
- draft report and a summary of the feedback provided by the entities involved in the assessment;
- the final report; and
- communications materials.

Deliverables from any follow-up conducted will depend on the extent of the follow-up.

6.0 LIMITATIONS OF ASSESSMENTS

It is important to keep in mind that any assessment will be limited in its applicability by its scope and objectives; the period of time captured in fieldwork; the specific areas of the entity that were assessed; the availability of applicable information; and the margin of error. Such details may limit the generalizability of assessment findings across the wider entity, other time periods, and other like entities.

As such, the final report should not be seen as a definitive account of an entity's total personal information handling practices; nor should the report be seen as an endorsement of the entity's compliance with its obligations under FIPPA or PIPA.

7.0 APPENDIX 1: LEGISLATIVE AUTHORITIES AND POWERS

Monitoring and Compliance (FIPPA s. 42 and PIPA s. 36)

With regard to the public sector, s. 42(1) outlines the Commissioner's responsibilities for monitoring how FIPPA is administered and states that the Commissioner may:

- investigate or audit to ensure compliance with any provision of this Act or regulation;
- make orders resulting from investigations or audits;
- receive comments from the public; and
- engage in or commission research into anything affecting the achievement of the purposes of the Act.

The corresponding section for the private sector organizations is s. 36(1) of PIPA. This section is similar to the above with the exception that the Commissioner may investigate or audit if there are reasonable grounds to believe that an organization is not complying. The Commissioner may also exchange information with other privacy Commissioners across Canada for the purpose of coordinating activities.

Assessments may comprise investigation, audit, research or any combination of the monitoring and compliance functions.

Inspection and Collection of Evidence (FIPPA s. 44 and PIPA s. 38)

Compel Records and Answers to Questions (FIPPA s. 44 and PIPA s. 38)
For the purposes of conducting an assessment, s. 44 of FIPPA and s. 38 of PIPA authorize the Commissioner to make an order requiring a person to answer questions or to produce a record, including a record containing personal information. The Commissioner may also apply to the Supreme Court for an order directing a person to comply with the Commissioner's order. These provisions also apply in situations where a record is subject to solicitor client privilege (such privilege is not affected by disclosing the record to the OIPC).

Entry and Inspection (PIPA s. 38)
Section 38(2) of PIPA also permits the Commissioner to enter any premises at any reasonable time (other than a personal residence) occupied by an organization after satisfying security requirements of the organization relating to the premises.

Protections (FIPPA ss. 30.3, 45–47 and PIPA ss. 39–41, 54–55)

People may have concerns about liability with regard to statements made to the OIPC during an assessment. There are sections in both FIPPA and PIPA that provide certain protections to individuals who have made statements or responded to questions asked by the OIPC.

Restrictions on Disclosure by Commissioner (FIPPA s. 47 and PIPA s. 41)
Sections 47(3) of FIPPA and 41 of PIPA contain a general prohibition against disclosure by the Commissioner and her staff related to any information obtained in performing their duties, powers and functions under the Acts. In addition, FIPPA s. 3 notes that FIPPA does not apply to records created by or for, in the custody or control of, or that relate to the exercise of the

Commissioner's functions. This means that the OIPC's operational records are not subject to access for information requests.

Evidence in Proceedings (FIPPA s. 47(2.1) and PIPA s. 39)
Section 47(2.1) of FIPPA and s. 39 PIPA state that the Commissioner or her staff must not give or be compelled to give evidence in a court or other proceedings in respect of information collected while performing their duties (again, except with regard to perjury, prosecution for an offence under the Acts, or in an application for judicial review or an appeal).

Protection Against Libel or Slander Actions (FIPPA s. 46 and PIPA s. 40)
Similarly, s. 46 of FIPPA and s. 40 of PIPA state that anything said, any information supplied or any record produced by a person during an investigation by the Commissioner is privileged in the same manner as if the investigation were a proceeding in a court.

Whistleblower Protection (FIPPA s. 30.3 and PIPA s. 54)
FIPPA s. 30.3 and PIPA s. 54 state that employers must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny that employee a benefit, because the employee has: disclosed to the Commissioner that any other person has contravened or is about to contravene this Act; has done or has intention of doing anything required in order to avoid a contravention of this Act; or has refused to do anything in contravention of this Act.

Reporting (FIPPA s. 42 and PIPA s. 36)

Sections 42 of FIPPA and 36 of PIPA allow the Commissioner to inform the public about the Act and comment on: implications for access or protection of privacy of legislative schemes, programs, activities of public bodies; protection of personal information of programs proposed by organizations; and automated systems or data-linking initiatives by public bodies or private sector organizations.

This includes public posting of reports or other materials that result from an OIPC assessment. Determinations of whether to inform the public about the results of an assessment, along with the type of information that may be shared, will be made on a case-by-case basis.

Delegation (FIPPA s. 49 and PIPA s. 43)

FIPPA s. 49 and PIPA s. 43 allows the Commissioner to delegate her duties, powers and functions to any person. One exception to the ability to delegate under FIPPA is that the Commissioner may not delegate the power to examine information referred to in s. 15 (disclosure harmful to law enforcement) if the head of a police force or the Attorney General has refused to disclose that information and has requested the Commissioner not to delegate the power to examine that information.

Responsibility for planning, conducting, reporting and following-up on Audit and Compliance Program assessments sits with the OIPC's Senior Investigator of Audit and Compliance and may also include other investigators, policy analysts, intake officers or assistant Commissioners.

Interactions with Other Legislation

There are no legislative provisions in other Acts that prevent the OIPC from accessing records and conducting assessments of public bodies or private sector organizations.