GENERAL

March 2026

Guide to OIPC audits, systemic investigations, and compliance reviews

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PURPOSE OF THIS DOCUMENT

This document is intended to assist public bodies and private sector organizations to better understand the OIPC's authority and function regarding audits, systemic investigations, and compliance reviews, and the basic procedural steps involved. This guide includes the most common procedures that the Office of the Information and Privacy Commissioner (OIPC) uses under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA) to conduct audits and systemic investigations.

Within its Audit & Systemic Review (AnSR) program, the OIPC conducts proactive audits, systemic investigations, compliance reviews, and other research projects. These projects often assess how effectively public bodies and private sector organizations protect personal information and comply with access provisions in FIPPA and PIPA.

AnSR projects may be proactive in nature or initiated in response to present or emerging access or privacy issues, often involving high-profile and complex investigations that are significant for guiding interpretation of legislation. The OIPC may conduct these projects alone or jointly with other provincial or federal regulators.

ANSR PROJECTS

To conduct AnSR projects, the OIPC draws from a combination of compliance verification, systemic investigation, operational audit, information management and technology audit, program evaluation, and process improvement methodologies. AnSR projects assess various aspects of access to information or privacy management, for example:

- **Governance, policies, procedures, and training**: Reviewing an entity's management of access to information or protection of privacy programs, access to information or privacy policies and procedures, information and data sharing agreements, and staff training related to access or privacy.
- **Collection, use, disclosure, and retention:** Assessing an entity's collection, use, disclosure and retention of personal information, determining whether appropriate notice is provided and meaningful consent obtained; and determining whether the entity limits collection, use, disclosure and retention of personal information to only what is necessary or reasonable for the program or business.
- **Protections and safeguards:** Examining an entity's access and disclosure provisions, and determining whether reasonable administrative, technical and physical safeguards are in place to protect personal information against risks, such as unauthorized access, collection, use, disclosure, or disposal.

- **Access to information:** Reviewing an entity's access to information processes, how it handles access-related requests or complaints, the time it takes to respond to access requests, and compliance with access-related obligations under FIPPA or PIPA.
- **Accountability and compliance monitoring:** Evaluating how an entity monitors its own compliance with privacy policies and procedures or legislation, handles privacy-related complaints, reviews safeguards, and manages breaches.

AnSR project reports are often published online (www.oipc.bc.ca/reports/investigation-and-audit-reports) and commonly identify areas where an entity may excel as well as areas where improvements are needed to comply with legislation and guidelines. Where improvements are needed, reports will contain recommendations to improve privacy or access to information practices, policies, guidelines, or legislation. These recommendations may be directed to a single entity, a broader group (such as an industry sector or public body type), or government.

KEY LEGISLATIVE AUTHORITY, POWERS, AND PROTECTIONS

The Commissioner has the following powers when conducting AnSR projects:

- investigate or audit entities to ensure compliance with any provision of these Acts or regulations (FIPPA s. 42 and PIPA s. 36);
- make orders resulting from investigations or audits (FIPPA s. 42 and PIPA s. 36);
- receive comments from the public (FIPPA s. 42 and PIPA s. 36);
- engage in or commission research into anything affecting the achievement of the purposes of the Acts (FIPPA s. 42 and PIPA s. 36);
- compel production of records and answers to questions (FIPPA s. 44 and PIPA s. 38);
- entry of premises and inspection of information (PIPA s. 38);
- inform the public about the Acts or comment on the implications for access to information or for protection of privacy of various matters (FIPPA s. 42 and PIPA s. 36); and
- delegate their duties, powers, and functions to any person (FIPPA s. 49 and PIPA s. 43).

Several sections in both FIPPA and PIPA provide certain protections to individuals who make statements to, or answer questions from, the OIPC during an AnSR project, including:

- general restriction on disclosure by the Commissioner and OIPC 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.

STEPS FOR ANSR PROJECTS

Step One: Planning

Identifying topics, entities, and scope

OIPC identifies and selects topics or entities for AnSR projects based on a variety of factors and resources, including:

- analysis of OIPC files such as complaints, requests for review, and breach reports received by the OIPC;
- media reports on access or privacy practices within a specific entity, sector or topic;
- consultation with FOI, privacy, and security experts, or other regulators;
- follow-up with entities involved in previous AnSR projects, particularly where there were recommendations for the entity to implement; and
- a need to explore a particular topic or sector for input into policy or legislative amendments.

Objectives of the reports are often geared toward measuring compliance but may also include contributing to a body of knowledge on a particular topic, updating OIPC guidance documents, recommendations for amendments to policy or legislation, or other purposes. The OIPC typically documents planning decisions in project charters or project plans.

Choosing methodology

The OIPC selects methodology based on the nature of the specific project and the circumstances of the topics or entities involved. The OIPC often uses a combination of the following methodologies:

- interviews with senior entity staff;
- interviews or group discussions with key program area staff;
- inspection of the entity's premises or 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);
- written submissions from an entity responding to OIPC questions, or submissions from others involved with the topic, program, or entity being assessed;
- file reviews (for example, an entity's FOI or complaint files, access logs, etc.);

- review of program materials or other documents (such as policies, contracts, memos, or other correspondence); and
- surveys to assess knowledge and awareness, program metrics (where there are multiple entities), or other topics.

Notifying the entity
The OIPC will notify an entity involved in an AnSR project in writing by sending a letter to the head of the entity. Such notification outlines the OIPC's intention to audit, investigate, or otherwise conduct research involving the entity. Additionally, the notification will outline the reasons why an entity or entities were selected for the project and its anticipated scope, methodology, and timelines.

Step Two: Background research and assessment criteria

Understanding the "lay of the land"
The success of AnSR projects often depends on cooperation from entity staff; access to systems, records, and information; and availability of evidence. As such, the OIPC may invite key entity staff to comment on challenges or issues they feel may interfere with successful completion of the project. In addition, the OIPC may consult with an entity before starting a project to gain a better understanding of the topics involved, the types of materials available, and the structure of the entity.

The OIPC may also make a preliminary request for information or materials, which may include:

- written polices or procedures;
- organizational charts and contact information for key staff;
- descriptions of safeguards employed to protect personal information;
- information sharing agreements, contracts, and work orders;
- privacy impact or risk assessments and project-related reports;
- a small sample of files that may be included in a file review;
- training materials and/or details regarding training programs, and memos or directives to staff; or
- communication materials regarding a program or service.

In addition, the OIPC may collect and analyze media, professional journal, or other articles on a particular topic or entity. Such documents can help develop an understanding of the topic, entity, or potential issues the project may encounter.

Building assessment criteria and tools
Assessment criteria are standards against which compliance can be evaluated and assessed. The OIPC selects or adapts criteria for each specific project. Criteria are to be relevant, unbiased, sufficiently fulsome, understandable and reliable. The most common resources used to develop assessment criteria include:

- FIPPA, PIPA, or other relevant legislation, regulations, directives or enactments;
- OIPC orders and court decisions;
- recommendations from previous investigations or audits (internal or external);
- guidance developed by other Privacy Commissioners or relevant oversight entities; and
- relevant entity policies, agreements, or contract terms relating to how personal information is managed.

Assessment tools are instruments used to collect, organize, and analyze data during an AnSR project. The OIPC will either build these tools in advance of a project and review or amend them prior to use or build them after reviewing background materials. The tools used will depend on the objectives of the project and will be developed from the criteria outlined above. Examples of such tools include:

- guides for use during interviews or group discussions;
- written questions to solicit information and requests for documents;
- inspection checklists for use during onsite examinations or review of electronic files;
- spreadsheets for reviewing entity files; and.
- questionnaires for conducting surveys.

Step Three: Fieldwork

Gathering and documenting evidence
Evidence can include any information the OIPC obtains during an AnSR project. For example, depending on the selected methodology, evidence can come from

- interviews;
- physical inspections and observations;
- written submissions;
- document, system, or file reviews; or
- surveys or questionnaires.

The OIPC often conducts interviews with key entity or program area staff. Such interviews help the OIPC gain knowledge about the entity, relevant programs or processes, and staff awareness. Interviews also assist the OIPC learn about topics being assessed and to corroborate

evidence. The OIPC will take notes and may digitally record interviews to ensure evidence is available for analysis and to substantiate conclusions drawn.

The OIPC will gather sufficient evidence to develop conclusions that are valid, objective, and logical, to the extent that a reasonable person may reach the same conclusions when reviewing the evidence. There may be occasions where the OIPC requests additional information beyond what was originally requested or sought. For example, the OIPC may seek additional records for review, or conduct follow-up interviews with staff to clarify points or ask additional questions.

The OIPC will document and maintain the evidence used to support its findings. This may include saving copies of relevant communications and background materials, initial assessment planning documents, interview or focus group notes, completed inspection or observation checklists, and aggregate findings from questionnaires or statistical analysis.

Sharing initial findings
The OIPC may provide an entity with feedback during an AnSR project. For example, the OIPC will often raise identified gaps or challenges during the collection and initial analysis of evidence with the management of the entity involved. Sometimes gaps or challenges may not be as obvious and will be identified during further analyses and included in the draft report. Where possible, the OIPC strives for open communication and continuous feedback, providing entities with opportunity to implement any improvement measures promptly. Ultimately, the goal is to improve privacy and access practices and support information and privacy rights of people in BC.

Step Four: Analysis and drafting

Analyzing results
The OIPC will analyze evidence collected against the assessment criteria established. 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 several questionnaires or to count the prevalence of a particular issue in a sample of files. The OIPC uses both qualitative and quantitative analysis to interpret whether the entity has met the assessment criteria, such as compliance with different aspects of FIPPA or PIPA. Analysis will reveal whether there is sufficient evidence to support an assessment finding.

Drafting the report and internal review
The OIPC summarizes findings in a summary report. The report usually includes, at minimum:

- a description of the entity and topic;
- an outline of the scope and criteria;
- a description of the methodology used;
- key findings and a summary of related evidence;

- a summary of gaps or challenges found and why these are important to address; and
- recommendations to address the gaps or challenges found.

The OIPC conducts several internal reviews of the report, which typically include the project team, Directors, Deputy Commissioners, and the Communications team. The report drafters incorporate internal feedback and submit a draft report to the Commissioner for review and approval.

Entity review
Once the report has been approved by the Commissioner, the OIPC shares an embargoed copy of the report with the entity involved. The entity is asked to provide feedback relating to any errors, omissions, or misinterpretations in the report. The entity can raise concerns with the OIPC, which will then review the feedback and determine what changes, if any, to incorporate in the final report.

Entities may also be asked to provide an official response to the report findings and whether they accept the OIPC's recommendations. If entities have already implemented or initiated some of the recommendations, the OIPC will consider updating the report to include a description of the amendments undertaken.

Step Five: Reporting

Finalizing report
The project team will provide the report to the Commissioner for a final review and approval of the report content. The Commissioner determines whether the report will be made public in part or in its entirety.

If not approved for public release, the report will be finalized and provided to the entity, typically along with a request for the entity to provide status updates within a given period on its implementation of any recommendations made by the OIPC.

Public release
If approved for publishing on the OIPC's website, the Communications team will edit the content and structure of the report, create the publishing design and layout, and create a series of media and other materials to accompany the report's publication. These additional materials are all subject to Commissioner approval and often include:

- media advisory;
- news release;
- key messages and Q&A for the Commissioner;
- infographic overview or fact sheet with report findings;
- video message from the Commissioner; and

- any related guidance published on the topic of the report.

Prior to public release, the OIPC sends the final copy of the report (or portion being published) to the entity involved, typically along with a request for the entity to provide status updates within a given period on its implementation of any recommendations made by the OIPC.

Media outlets may request the Commissioner participate in radio or television interviews, or to provide written responses to questions regarding the report, its findings and recommendations, or related topics.

Step Six: Follow-up on recommendations

The OIPC reviews status updates provided by the entity and determines whether the actions taken meet the recommendations included in the report. The OIPC documents implementation in the project folder and continues to follow-up with the entity as necessary until satisfied with the implementation.

Occasionally, the OIPC may conduct a more formal follow-up investigation to determine the level of compliance with the recommendations or the assessment criteria and may draft a report. These follow-up reports may also be published on the OIPC's website and would follow similar steps taken for the original report when it comes to fieldwork, analysis, drafting, and reporting.

If the OIPC is not satisfied with the implementation of the recommendations from a report, or if an entity has indicated that they do not intend to implement the recommendations, the Commissioner or their delegate may issue an order to ensure compliance with the Acts. Such orders are legally binding, are enforceable by a court of law, and are subject to judicial review by the BC Supreme Court.

APPENDIX 1: LEGISLATIVE AUTHORITIES AND POWERS

Monitoring and compliance (FIPPA s. 42 and PIPA s. 36)
In the context of public bodies, FIPPA s. 42 states that the Commissioner is generally responsible for monitoring how FIPPA is administered and may:

- investigate or audit to ensure compliance with any provision of FIPPA or the 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 FIPPA.

Regarding organizations, PIPA s. 36 sets out similar authorities and powers to FIPPA, with the exception that the Commissioner may investigate or audit if there are reasonable grounds to believe that an organization is not complying with PIPA. The Commissioner may also exchange information with other privacy Commissioners across Canada for the purpose of coordinating activities.

Compel records and answers to questions (FIPPA s. 44 and PIPA s. 38)
For the purposes of conducting an audit or investigation, FIPPA s. 44 and PIPA s. 38 authorize the Commissioner to order 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. Such orders may also include orders for procedural matters, for example, an order to produce a record for the OIPC's examination where that order is issued under FIPPA s. 44.

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

The Commissioner may examine any information in a document, including personal information, and obtain copies or extracts of documents containing information found in any premises the Commissioner enters, or is otherwise provided to the Commissioner under PIPA.

Protections (FIPPA ss. 30.3, 45–47 and PIPA ss. 39–41, 54–55)
People may have concerns about liability regarding statements made to the OIPC during an AnSR project. 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.

FIPPA s. 30.3 and PIPA s. 54 protect employees from retaliatory action by an employer who, when acting in good faith and with reasonable belief, attempts or may attempt to prevent a contravention of either Act, or discloses to the Commissioner that the employer or any other person has contravened or is about to contravene either Act.

Restrictions on disclosure by Commissioner (FIPPA s. 47 and PIPA s. 41)
FIPPA s. 47 and PIPA s. 41 contain a general prohibition against disclosure by the Commissioner and their staff related to any information obtained in performing their duties, powers and functions under the Acts. There are exceptions, however, such as where disclosure is necessary to conduct an investigation, audit or inquiry under the Acts, or to establish the grounds for findings and recommendations contained in a report.

In addition, 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 to information requests.

Evidence in proceedings (FIPPA s. 47(2.1) and PIPA s. 39)
FIPPA s. 47(2.1) and PIPA s. 39 state that the Commissioner or their 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, except in limited circumstances listed in FIPPA s. 47(2.2).

Protection against libel or slander actions (FIPPA s. 46 and PIPA s. 40)
Similarly, FIPPA s. 46 and PIPA s. 40 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 ss. 54-55)
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 the Act, has done or has intention of doing anything required in order to avoid a contravention of the Act, or has refused to do anything in contravention of the Act.

Further, PIPA s. 55 allows a person who notifies the Commissioner about a contravention of PIPA to request that the Commissioner keep the person's identity confidential with respect to the notification.

Reporting (FIPPA s. 42 and PIPA s. 36)
FIPPA s.42 and PIPA s. 36 allow the Commissioner to inform the public about the Acts and comment on:

- implications for access or protection of privacy of legislative schemes (FIPPA);
- programs, activities of public bodies (FIPPA);
- protection of personal information of programs proposed by organizations (PIPA); and

- automated systems or data-linking initiatives by public bodies or private sector organizations (FIPPA and PIPA).

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

Delegation (FIPPA s. 49 and PIPA s. 43)
Generally, FIPPA s. 49 and PIPA s. 43 allows the Commissioner to delegate their duties, powers and functions to any person. A list of current delegations made under each Act is available on the OIPC website.

One exception under FIPPA is that the Commissioner may not delegate the power to examine information referred to in FIPPA 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.

The Director of AnSR, along with support from other OIPC staff, is generally responsible for planning, conducting, and reporting on AnSR projects, and performing follow-up as needed.

Interactions with other legislation
There are no legislative provisions in other Acts that prevent the OIPC from accessing records and conducting AnSR projects relating to public bodies or private sector organizations.