

OIPC/ORL Privacy Management Audit Plan

The Privacy Officer for the Office of the Information and Privacy Commissioner (OIPC) and the Office of the Registrar of Lobbyists (ORL) monitors and oversees the effectiveness of OIPC/ORL program controls and revises or improves them as necessary.

Part of the Privacy Officer's duties include conducting (or assigning staff to conduct) annual audits of the OIPC/ORL privacy management program. Audits will typically include examination of program controls within the following areas:

1. Personal information inventories,
2. Privacy and other applicable policies,
3. Privacy impact assessments and security threat and risk assessments,
4. Staff training and education,
5. Privacy and information security safeguards,
6. Breach and incident management response protocols,
7. Requirements in contracts with service providers, and
8. External communication explaining privacy policies.

The purpose of the audits is to confirm that program controls remain effective and to identify areas that require attention. Audits are conducted using tools and methodology established by the Privacy Officer and assigned staff.

Such methodology includes, for example:

- A review of the previous audit report and recommendations,
- Interviews with or emailed questions and responses from the Privacy Officer and Directors,
- A review of Privacy Management Plan documents and policies,
- A review of training materials and risk assessments, and
- A survey to staff relating to security safeguards.

Each audit will conclude with a report that: confirms the scope and methodology of the audit; identifies key findings (including any threats or risks), confirms implementation of recommendations from the previous year's audit (if applicable), and makes new recommendations, as necessary, to address issues identified during the audit.

If an audit identifies a concern with OIPC/ORL program controls, the Privacy Officer will identify and coordinate with the appropriate person(s) to address the concern and follow up accordingly.

Information systems program controls

The Privacy Officer will be in contact with the Corporate Shared Services Privacy Officer to confirm that adequate controls are in place for systems that contain personal information. This may include reviewing reports and findings from any internal or external audit of IT systems. OIPC/ORL reserves the ability to conduct its own audit of systems as necessary.

ADMINISTRATIVE POLICIES AND PROCEDURES Office of the Information and Privacy Commissioner Office of the Registrar of Lobbyists	
Subject: OIPC/ORL Privacy Management Audit Plan	Date Issued: March 3, 2016 Date revised: January 6, 2026

This document is for information purposes only and does not constitute a decision or finding by the Information and Privacy Commissioner and Registrar of Lobbyists for British Columbia, or their delegate(s). This guidance does not affect the powers, duties, or functions of the Information and Privacy Commissioner and Registrar of Lobbyists, or their delegate(s), regarding any complaint, investigation, or other matter under the *Freedom of Information and Protection of Privacy Act*, the *Personal Information Protection Act*, or the *Lobbyists Transparency Act*.