JANUARY 2026

AI Guidance for Canadian Organizations Assessment Pack

Regulator ready governance baseline that explicitly “grounds assessment” of AI adoption against privacy and human rights obligations.

Authority and source basis

This Assessment Pack is grounded in the “IPC and OHRC Principles for the Responsible Use of Artificial Intelligence” (January 2026), jointly developed by the Office of the Information and Privacy Commissioner of Ontario (IPC) and the Ontario Human Rights Commission (OHRC).

The IPC and OHRC state these principles “will ground our assessment of organizations’ adoption of AI systems consistent with privacy and human rights obligations.” Standards and frameworks explicitly referenced up front in the guidance

The document positions the IPC and OHRC principles as complementary to major provincial, national, and international initiatives, including:

- European Union (EU) Ethics Guidelines for Trustworthy AI G7 Hiroshima Process,
- International Guiding Principles for Organizations Developing Advanced AI Systems

OECD AI Principles

The guidance adopts Ontario’s Enhancing Digital Security and Trust Act (EDSTA) definition of an AI system, and notes it is consistent with the OECD definition.

ISO 42001 note

The IPC and OHRC document pack does not explicitly reference ISO/IEC 42001. However, it is designed to operationalize governance principles into implementable controls and supporting documentation that can be mapped to an AI Management System (AIMS).
When used as part of an organization’s broader management system approach, the pack can be positioned as a “principles to controls” bridge that supports alignment with ISO/IEC 42001.

What this Assessment Pack helps an organization do

This Assessment Pack supports organizations to implement responsible AI governance by enabling them to:

- Establish an AI governance baseline that is explicitly framed by Ontario’s privacy and human rights commissioners as assessment-ready.
- Apply the principles across the full AI life cycle (design to decommissioning), not just deployment.
- Produce defensible documentation for transparency, oversight inquiries, and corrective action readiness.

Intended scope

Use this pack to assess any AI system (including genAI) that produces outputs used for decisions, recommendations, or content. This includes systems that influence business or operational outcomes, whether directly (automated decisions) or indirectly (decision support), and whether the outputs are internal (staff facing) or external (customer facing).

Life cycle coverage expected by the guidance

Controls should be assessed across the full AI lifecycle, with expectations tailored to the activities and risks present at each stage:

- Design, data, modelling
- Verification and validation
- Deployment
- Operation and monitoring
- Decommissioning and retention as lawfully required Role clarity

In practice, organizations may hold multiple roles at once (for example, configuring a vendor model for a specific workflow). In these cases, the assessment should document the organization's role at each stage and apply the corresponding control expectations.

Assessment outputs

- **Principles Alignment Scorecard** (by principle, by life cycle stage)
- **Evidence Register** (what exists, what is missing, what is weak)
- **Control Gap List** (prioritized, with owners and target dates)
- **Board-ready Summary** (key risks, top remediation actions, readiness narrative)

Scoring method

Score each control 0 to 3:

- **0 Not present:** no evidence
- **1 Partial:** informal or incomplete evidence
- **2 Implemented:** documented and operating
- **3 Mature:** tested, monitored, and improved over time

Evidence request list (minimum viable “proof pack”)

For each AI system in scope, obtain and review the following supporting documentation:

1. **System identification and classification:** AI system inventory entry, role (developer, provider, user), purpose, and risk tier
2. **Validity and reliability evidence:** testing results and the testing standard used
3. **Safety and security controls:** safety monitoring plan, including resilience to unexpected events and deliberate harm, and cybersecurity safeguards
4. **Privacy by design and lawful authority:** privacy by design evidence, lawful authority, minimization approach, and PETs used (de-identification, synthetic data)
5. **Human rights and discrimination safeguards:** human rights and discrimination risk assessment artifacts, plus monitoring for bias and mitigation actions
6. **Transparency and traceability:** public account, notices, explainability method, traceability records
7. **Governance artifacts:** oversight roles, human in the loop procedures, risk assessments (privacy, human rights, algorithmic impact)
8. **Complaint, challenge, and FOI readiness:** complaint and challenge mechanism and FOI response process
9. **Decommissioning and retention:** decommissioning criteria, shutdown procedure, and retention plan for outputs and data as lawfully required

The six principles (assessment domains)

The principles are stated as interconnected and equally important, and should be applied as a unified set, rather than treated as standalone requirements or implemented in isolation:

- **Accountable**
- **Valid and Reliable**
- **Safe**
- **Privacy Protective**
- **Human Rights Affirming**
- **Transparent**

Checklist and Control Library

Below is a usable checklist and a corresponding control set. To turn this tracking checklist into a scoring worksheet, ask your Risk Advisor or copy the Control List into a spreadsheet.

A) Governance and accountability controls (Accountable)

A1. Governance and ownership

- [ ] C-A01 Named accountable owner(s) for each AI system, with authority to pause or decommission systems that become unsafe or not valid/reliable.
- [ ] C-A02 Clearly defined roles, responsibilities, oversight procedures, including a human-in-the-loop approach for real-time intervention

A2. Risk assessment

- [ ] C-A03 Up-front risk assessments completed, including privacy and human rights impact assessments, algorithmic impact assessments, and others as appropriate.

A3. Documentation, recourse, oversight

- [ ] impacted groups are meaningfully informed and can challenge outputs and seek recourse.
- [ ] C-A05 Ability to explain the AI system to an independent oversight body, with plain language documentation; corrective action process exists and is usable.
- [ ] C-A06 Mechanism to receive and respond to privacy, transparency, and human rights concerns, plus freedom of information requests and decision challenges.

A4. Whistleblowing and enforcement posture

- [ ] C-A07 Safe whistleblowing protections, including the ability to report non-compliance to independent oversight without reprisal.
- [ ] C-A08 Review readiness for oversight body enforcement and directed remedial or corrective actions.

B) Validity and reliability controls (Valid and reliable)

- [ ] C-VR01 Independent testing standards defined for intended use; objective evidence shows requirements are fulfilled.

- [ ] C-VR02 Reliability evidence shows consistent performance over the required duration and environment of use.
- [ ] C-VR03 Robustness testing covers varied operating conditions, including contexts where outcomes differ across communities.
- [ ] C-VR04 Data quality controls exist to detect inaccurate, biased, incomplete inputs; mitigations are defined.
- [ ] C-VR05 Validity and reliability assessment completed prior to deployment and repeated throughout the life cycle.

C) Safety and security controls (Safe)

- [ ] C-S01 Safety monitoring plan covers the full life span; evaluation confirms resilience to unexpected events and deliberate harmful efforts.
- [ ] C-S02 Cybersecurity protections are robust and appropriate to the system risk.
- [ ] C-S03 New use or new context triggers a comprehensive reassessment before use.
- [ ] C-S04 System makes evident when it is producing unexpected outputs; escalation and containment steps are defined.
- [ ] C-S05 Kill switch and decommissioning criteria exist; negative impacts to individuals and groups are reviewed.

D) Privacy controls (Privacy protective)

- [ ] C-P01 Privacy by design approach documented from the outset, including proactive privacy and security measures and right of access support where relevant.
- [ ] C-P02 Clear lawful authority documented to collect, process, retain, and use personal information; compliance with applicable privacy laws and directives.
- [ ] C-P03 Collection and use limited to what is required; PETs used to reduce dependence on large volumes of personal information (de-identification, synthetic data).
- [ ] C-P04 Training data bias is addressed to ensure accuracy of outputs, especially for consequential decisions or inferences.
- [ ] C-P05 Individuals are informed whether and when their personal information is used, and the purpose and intended use of the AI system.
- [ ] C-P06 Access and correction pathway exists for personal information, including information generated about them by an AI system, where appropriate.
- [ ] C-P07 Review rights exist for lower-risk automated decisions; opt-out to a human decision maker exists for high-risk automated decisions that materially impact well-being.
- [ ] C-P08 Security safeguards protect personal information against unauthorized access or misuse across the AI life cycle.

E) Human rights controls (Human rights affirming)

- [ ] C-HR01 Systemic discrimination risk is assessed on Ontario Human Rights Code protected grounds; mitigation actions are defined.
- [ ] C-HR02 Ongoing monitoring exists for discriminatory impacts; training data is adjusted when biases are detected.
- [ ] C-HR03 Deployment suitability checks avoid “uniform use” that can create adverse impact discrimination for diverse groups.
- [ ] C-HR04 Where applicable to governmental actors, Charter-aware safeguards prevent undue targeting of public or social movement participants and avoid disproportionate surveillance impacts.

F) Transparency and traceability controls (Transparent)

- [ ] C-T01 Public account exists describing system operation across the life cycle (design through decommissioning), written clearly and accessibly.
- [ ] C-T02 Transparency includes sources of personal data, intended purposes, how it is used, and how outputs may affect individuals or communities.
- [ ] C-T03 Individuals are notified when interacting with AI and when information presented has been AI-generated.
- [ ] C-T04 Understandability is supported by retaining sufficient technical information to explain decisions and why errors may occur.
- [ ] C-T05 Explainability requirement: ability to describe both “how” and “why” outputs are generated, scaled to the audience.
- [ ] C-T06 Traceability artifacts retained: model details, training and validation data details, and monitoring metrics, failures, periodic evaluations.

Optional add-on: Impact assessment accelerators (authoritative tie-in)

The guidance explicitly points to impact assessments as a leading strategy, and references both the OHRC Human Rights AI Impact Assessment and the IPC Privacy Impact Assessment Guide.

Visit www.PrivacyManagement.ca and www.PrivacyImpactAssessment.ca for help completing organization-wide PIAs and risk assessments, including the above checklist. A Privacy Risk Advisor will be happy to help