

A Practical AI Workflow Risk Register for Canadian Small Businesses

A lightweight workbook for attaching AI risk to a named workflow, owner, data boundary, control, approval and review trigger.

HOW TO USE THIS TOOL

- 01 Register the real workflow and consequence, not only the model.
- 02 Map data, affected people and concrete failure modes before use.
- 03 Assign testable controls, human authority and rollback evidence.
- 04 Review again after incidents or material workflow changes.

Educational operating tool only. It is not legal, privacy, employment, security or regulatory advice and is not a certification. Requirements depend on the organization and use case.

Workflow intake

Describe the real task, consequence and accountable owner before selecting a model or vendor.

WORKFLOW NAME	BUSINESS OWNER
INTENDED PURPOSE	AFFECTED PEOPLE
INPUT SOURCE	OUTPUT / ACTION
MODEL / VENDOR	DEPLOYMENT CONTEXT

- ☐ The intended purpose is necessary, specific and measurable.
- ☐ A non-AI or lower-risk method was considered.
- ☐ The output and following action are clearly separated.
- ☐ An accountable person can pause or reject the workflow.
- ☐ Customer-facing AI use and material decision support will be disclosed where appropriate.

Success measure and unacceptable outcome

Data and vendor boundary

Map data class, retention, training use, access and deletion before information enters a prompt.

DATA / INPUT	CLASS	NECESSARY?	STORED WHERE	TRAINING USE?	RETENTION / DELETE
	Public / internal / confidential / personal / sensitive				
	Public / internal / confidential / personal / sensitive				
	Public / internal / confidential / personal / sensitive				
	Public / internal / confidential / personal / sensitive				
	Public / internal / confidential / personal / sensitive				
	Public / internal / confidential / personal / sensitive				

- ☐ Vendor terms, data location, access, subprocessors and incident process reviewed.
- ☐ Personal or confidential data is removed, minimized or specifically authorized.
- ☐ Logs and outputs follow the organization's retention and deletion rules.
- ☐ A manual path exists if the vendor, integration or model becomes unavailable.

Failure-mode register

Describe concrete failures in this workflow, who could be affected and whether the harm is reversible.

ID	FAILURE MODE	AFFECTED PARTY	LIKELIHOOD 1-5	IMPACT 1-5	EXISTING CONTROL
AI-01					
AI-02					
AI-03					
AI-04					
AI-05					
AI-06					
AI-07					
AI-08					

Consider evidence, privacy, confidentiality, fairness, security, agency, operational continuity, disclosure and reputation.

Risk matrix and priority

Use the score to prioritize review - not to create false precision or waive accountability.

IMPACT / LIKELIHOOD	1 RARE	2 UNLIKELY	3 POSSIBLE	4 LIKELY	5 ALMOST CERTAIN
5 Severe	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Minimal	1	2	3	4	5

BAND	WORKING TREATMENT	WHO APPROVES
1-4 Lower	Document controls and owner; monitor in normal operations.	Workflow owner
5-9 Moderate	Test controls and approve with a scheduled review.	Owner plus reviewer
10-14 High	Redesign or constrain; require senior approval and monitoring.	Accountable executive
15-25 Critical	Do not deploy until risk is materially reduced.	Accountable executive

Adapt thresholds to the organization. Consequential legal, employment, health, finance or access decisions require qualified review regardless of a simple score.

Control and test plan

Make every control observable, assign an owner and define the evidence required before approval.

RISK ID	CONTROL / RESTRICTION	TEST CASE	PASS CRITERION	OWNER	EVIDENCE / DATE

[] Permitted data, tools, recipients and actions are technically bounded.

[] Representative, adversarial and known-failure tests are included.

[] Human reviewer sees the source, uncertainty and consequence.

[] Monitoring threshold and manual fallback are tested.

[] Rollback can disable the workflow without losing required records.

Approval and residual risk

Record the decision, conditions, evidence and human authority that remain after controls are applied.

DECISION: APPROVE / CONDITIONAL / PILOT / REDESIGN / STOP 	DECISION DATE
ACCOUNTABLE APPROVER 	INDEPENDENT REVIEWER
RESIDUAL RISK SUMMARY 	CONDITIONS BEFORE USE

- [] Public claims and high-impact decisions retain named human approval.
- [] The reviewer can reject output without being penalized for delay.
- [] Users have an escalation, correction or recourse path where relevant.
- [] Monitoring, incident response and rollback owners are active.
- [] The next review date and change triggers are recorded.

Approval evidence and signatures

Monitoring, incidents and change review

Reassess after failures and material changes to purpose, data, model, prompt, integrations or authority.

DATE	SIGNAL / INCIDENT	IMPACT	CONTAINMENT	OWNER	FOLLOW-UP

[]

Model, vendor, prompt, data source or tool permissions changed.

[]

The audience, purpose or downstream action expanded.

[]

Accuracy, correction, complaint or override rate crossed its threshold.

[]

A privacy, security, fairness or public-claim incident occurred.

[]

The manual fallback or rollback failed a test.

[]

A legal, contractual or regulatory requirement changed.

Sources: Office of the Privacy Commissioner of Canada AI and privacy guidance; ISED Voluntary Code of Conduct; NIST AI Risk Management Framework Core.