Vendor Evaluation Checklist

Canadian-Specific AI Tool Assessment

Vendor / Tool Name

Vendor Website

Evaluator Name

Date of Evaluation

Purpose This checklist evaluates any AI tool against Canadian regulatory requirements and compliance best practices. It is vendor-neutral and works for meeting documentation tools, portfolio analytics, client communication tools, research tools, or any AI application in financial advisory practice.

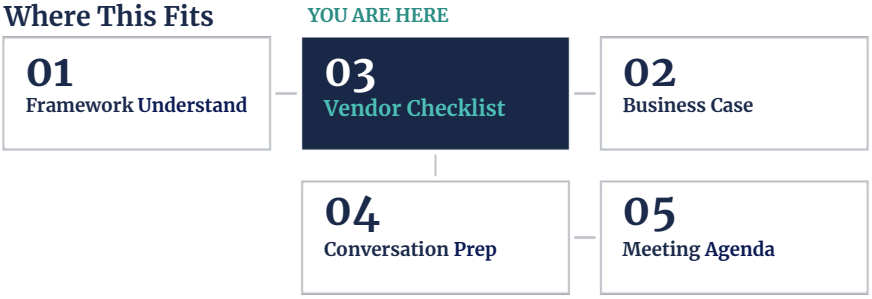
How to Use This Component

For each item, mark the tool's status. Where the answer is unclear or requires further investigation, mark "Unknown" and note what information is needed. An "Unknown" is better than an inaccurate response.

Sources: note where you found the information (vendor website, vendor representative, vendor documentation, independent verification).

Fields with a teal left border are the essentials. Complete at least these to get a basic assessment.

Where This Fits



This checklist helps you prepare for conversations about AI tool adoption at your firm. It does not constitute compliance or legal advice. Consult your firm's compliance department and legal counsel for guidance specific to your situation. Information in this kit reflects the regulatory landscape as of March 2026. Regulations and guidance are evolving.

Section 1 — Data Handling & Privacy

1.1 Where is client data stored at rest?

- ○ Canada
- ○ United States
- ○ Other (specify):
- ○ Unknown

Specific location/region if known:

1.2 Where does AI processing/inference occur?

Processing location may differ from storage location.

- ○ Canada
- ○ United States
- ○ Other (specify):
- ○ Unknown

1.3 Is personally identifiable information (PII) transmitted to external servers?

- ○ Yes
- ○ No
- ○ Partially (specify):
- ○ Unknown

> **Guidance**
> This is the critical question. If PII is transmitted, how is it protected? If PII is removed before transmission, how and where does that removal happen? The answer to this question shapes the entire compliance conversation.

1.4 How is PII handled?

Select all that apply.

- ☐ PII removed on advisor's device before transmission
- ☐ PII removed on vendor's servers
- ☐ PII encrypted in transit
- ☐ PII encrypted at rest
- ☐ No PII handling specified
- ☐ Unknown

1.5 Does the vendor retain client data after processing?

- ○ Yes (specify duration):
- ○ No
- ○ Unknown

If yes, can data be deleted on request?

○ Yes ○ No ○ Unknown

1.6 Is client data used to train AI models?

- ○ Yes
- ○ No
- ○ Unknown
- ○ Opt-out available

Section 1 — continued

Going Deeper:

1.7 What encryption is used for data in transit?

E.g., TLS 1.2, TLS 1.3, unknown.

1.8 What encryption is used for data at rest?

E.g., AES-256, unknown.

1.9 Does the vendor have a published privacy policy that addresses Canadian requirements?

- ○ Yes (link):
- ○ No
- ○ Unknown

1.10 Breach notification: what is the vendor's process?

SECTION 1 SUMMARY

Section risk rating

○ Low Risk ○ Medium Risk ○ High Risk ○ Cannot Assess

Section notes:

Section 2 — CIRO & Regulatory Alignment

2.1 Can tool outputs be exported for compliance record keeping?

- Yes (formats):
- No
- Partial
- Unknown

2.2 Do tool outputs support supervisory review?

A supervisor or compliance officer should be able to review what the tool produced and the inputs that generated it.

- Yes
- No
- Unknown

2.3 Does the tool maintain an audit trail?

- Yes No
- Partial
- Unknow
- n

2.4 Can the tool's outputs be retained for 7+ years?

CIRO IDPC Rule 3800 requires 7-year retention of business records.

- Yes (in-tool)
- Yes (via export)
- No Unknown
-

2.5 Does the tool support human-in-the-loop review before output is used?

CSA Staff Notice 11-348 recommends human oversight for AI systems affecting client services.

- Yes (required by tool)
- Yes (optional) No
- Unknown
-

2.6 Is the tool's decision-making process explainable?

CSA Staff Notice 11-348 encourages AI systems with high levels of explainability.

- Yes
- Partially
- No
- Unknown

If partially, what is explainable and what is not?

Section 2 — continued

2.7 Has the tool been used by other CIRO-regulated firms?

- ○ Yes (firms/count if known): _____
- ○ No
- ○ Unknown
- ○ Vendor will not disclose

2.8 Does the vendor provide compliance documentation?

Documentation that a compliance officer could use to support their evaluation.

- ○ Yes (describe): _____
- ○ No Unknown
- ○

SECTION 2 SUMMARY

Section risk rating

○ Low Risk ○ Medium Risk ○ High Risk ○ Cannot Assess

Section notes:

Section 3 — Security Posture

3.1 Does the vendor hold SOC 2 certification (Type I or Type II)?

- ○ Yes — Type I
- ○ Yes — Type II
- ○ No
- ○ Pending
- ○ Unknown

> **Certification Attribution**
> Distinguish between vendor certifications and infrastructure provider certifications. If the vendor says "SOC 2 certified," ask whether that is the vendor's own certification or their cloud provider's (e.g., AWS, Azure). A vendor built on AWS can say "Built on AWS, which maintains SOC 2." The vendor cannot claim SOC 2 certification unless they hold it independently.

3.2 Does the vendor hold ISO 27001 certification?

- ○ Yes
- ○ No
- ○ Pending
- ○ Unknown

Same attribution guidance as 3.1. Distinguish vendor-held from infrastructure-provider certifications.

Section 3 — continued

3.3 What cloud infrastructure does the tool use?

- ☐ AWS
- ☐ Azure
- ☐ Google Cloud
- ☐ Private infrastructure
- ☐ Unknown

Canadian region available?

◯ Yes ◯ No ◯ Unknown

3.4 Does the vendor have a published security policy?

◯ Yes (link): _____
◯ No
◯ Unknown

3.5 Does the vendor conduct regular security assessments?

◯ Yes
◯ No
◯ Unknown

3.6 Does the vendor carry cybersecurity insurance?

◯ Yes
◯ No
◯ Unknown

3.7 Access controls: how is advisor data isolated from other users?

Multi-tenant security. How does the vendor prevent other customers from accessing your data?

SECTION 3 SUMMARY

Section risk rating

◯ Low Risk ◯ Medium Risk ◯ High Risk ◯ Cannot Assess

Section notes:

Section 4 — Vendor Stability & Contractual

4.1 How long has the vendor been operating?

4.2 What is the vendor's funding/ownership structure?

VC-funded, bootstrapped, public company, subsidiary, etc.

4.3 How many financial advisory clients does the vendor serve?

4.4 What happens to your data if the vendor discontinues?

Data portability, export options, deletion guarantees.

4.5 Does the contract include a service level agreement (SLA)?

- ○ Yes (uptime guarantee):
- ○ No
- ○ Unknown

4.6 What are the contract terms?

Minimum commitment:

Cancellation notice:

Price lock period:

Section 4 — continued

4.7 Does the contract include a Canadian law governing clause?

- ○ Yes (province): _____
- ○ No
- ○ Unknown

4.8 Does the vendor accept a data processing agreement (DPA)?

- ○ Yes
- ○ No
- ○ Unknown

SECTION 4 SUMMARY

Section risk rating

○ Low Risk ○ Medium Risk ○ High Risk ○ Cannot Assess

Section notes:

Section 5 — Practical Evaluation

5.1 Have you personally tested the tool?

- ○ Yes (trial period): _____
- ○ No
- ○ Scheduled

5.2 Does the tool integrate with your existing technology?

Select all that apply.

- ☐ CRM (specify): _____
- ☐ Email (Outlook / other)
- ☐ Calendar
- ☐ Document management
- ☐ Portfolio system
- ☐ None assessed yet

Section 5 — continued

5.3 What training is required?

- ○ None
- ○ Self-guided tutorial
- ○ Vendor-provided training
- ○ Significant onboarding

5.4 Output quality assessment (if tested)

Rate each criterion from 1 (poor) to 5 (excellent). Leave blank if not tested.

Criterion	Rating (1–5)
Accuracy	
Relevance	
Professional quality	
Compliance documentation standards	

Quality notes:

5.5 Would you be comfortable showing this tool's output to a compliance officer?

Thisisapracticalconfidence test. If the answer is "no" or "with modifications," note what would need to change.

- ○ Yes
- ○ With modifications
- ○ No
- ○ Have not tested

If "withmodifications," specify:

SECTION 5 SUMMARY

Section risk rating

○ Low Risk ○ Medium Risk ○ High Risk ○ Cannot Assess

Section notes:

Section 6 — Overall Assessment

SUMMARY RISK TABLE

Evaluation Area	Section Rating	Key Concern	Acceptable?
Data Handling & Privacy			○ Y ○ N ○ C
CIRO & Regulatory			○ Y ○ N ○ C
Security Posture			○ Y ○ N ○ C
Vendor Stability			○ Y ○ N ○ C
Practical Evaluation			○ Y ○ N ○ C

(C = With Conditions)

Overall vendor risk rating

- ○ Low (recommend proceeding)
- ○ Medium (proceed with conditions)
- ○ High (significant concerns to resolve)
- ○ Do not recommend

Conditions for proceeding (if Medium)

What must be resolved or mitigated before proceeding.

Key strengths of this vendor (top 3–5)

Key risks or gaps (top 3–5)

Recommended next steps

- ☐ Proceed to Business Case (Component 02)
- ☐ Request additional vendor information
- ☐ Compare with alternative vendor
- ☐ Seek compliance guidance before proceeding
- ☐ Do not proceed

Evaluator: **Date:**

> **Guidance** If you are comparing multiple vendors, complete a separate checklist for each tool. The summary risk table on this page allows side-by-side comparison across vendors.