AI Compliance Readiness Checklist

A practical, step-by-step tool to assess current AI practices and spot gaps in governance or risk management

September 2025

DISCLAIMER: This AI Compliance Checklist is provided as a general recommendation only. It should not be considered legal advice. Organizations are strongly encouraged to review and adapt this checklist in consultation with their Chief Information Security Officer (CISO), legal counsel, or compliance team before implementation.

Contents

1) Leadership & Accountability

Define who is on the hook for AI risk. Keep the conversation on every exec agenda, not just when a tool is launched.

☐ Name a senior accountable owner (e.g., COO, GC, CISO) with clear authority and budget.

☐ Document reporting lines to the Board or Risk Committee; include AI on quarterly dashboards.

☐ Approve an AI control set (Acceptable Use, Model Risk, Vendor, Retention, Secure Prompting).

☐ Maintain an AI Register covering firm-built tools, SaaS features (e-signature, e-discovery), and plug-ins.

☐ Map AI risks into the enterprise risk taxonomy with appetite thresholds and triggers.

Notes / decisions: _____

2) Use-Case Register & Triage

Not every AI use is equal. Start with a list; rate each for impact and sensitivity.

☐ Catalogue use cases across practice groups (litigation support, tax prep, audit analytics, KM).

☐ Tag personal data and privilege exposure; flag client-specific or regulated data sets.

☐ Rate inherent risk (privacy, fairness, safety, financial, reputational); assign control tiers.

☐ Run PIA/DPIA where personal or inferred data is involved; record mitigations.

Notes / decisions: _____

3) Data & Privacy (Law 25, CPPA/PIPEDA)

Tighten data hygiene before prompts ever reach a model.

☐ Update transparency notices and lawful basis where prompts or outputs process personal data.

☐ Enforce minimization in prompts; set retention for logs, outputs, and training/eval sets.

☐ Apply de-identification/psedonymization and encryption in transit/at rest for sensitive data.

☐ Assess cross-border transfers; use SCCs/contractual clauses and, where feasible, localization.

☐ Operationalize subject rights: access/correction/explanation for AI-assisted decisions.

Notes / decisions: _____

4) Model & System Lifecycle

Treat models like systems that change over time—because they do.

☐ Track provenance and version history; keep a simple model bill of materials (MBOM).

☐ Pre-deployment tests: bias/accuracy/toxicity/robustness and targeted red-teaming.

☐ Keep humans in the loop for high-impact automation affecting client outcomes.

☐ Maintain decision rationale and explainability summaries where decisions affect rights.

☐ Change-management with rollback criteria, approvals, and release notes.

Notes / decisions: _____

5) Security & Resilience

Assume curious prompts and creative attackers.

☐ Mitigate prompt-injection, data exfiltration, and retrieval abuse; sanitize inputs/outputs.

☐ Isolate secrets and API keys; set sensible rate limits and anomaly detection.

☐ Log model interactions and drift; alert on jailbreak attempts and unusual outputs.

☐ Test backup/DR for datasets, vector stores, and model artifacts; rehearse restore.

☐ Schedule independent security testing and AI red-team exercises.

Notes / decisions: _____

6) Third-Party & Vendor Risk

Your exposure includes the models and platforms you don't control.

☐ Contract for data boundaries (no training on your data, IP protections, deletion on exit).

☐ Review SOC 2/ISO 27001 attestations and privacy commitments; record incident histories.

☐ Perform third-party model risk reviews and refresh them on a defined cadence.

☐ Plan the off-ramp: data return/deletion, model portability, and service continuity.

Notes / decisions: _____

7) Responsible AI & Ethics

Principles are helpful only if they steer real decisions.

☐ Adopt measurable principles (fairness, accountability, transparency) and define how to test them.

☐ Design bias mitigation plans; test protected-class impacts on key workflows.

☐ Publish a simple harm-reporting channel (e.g., an ethics inbox) and track triage times.

☐ Consider accessibility/inclusion in AI-enabled client services and portals.

Notes / decisions: _____

8) Operations & Monitoring

If you can't see it, you can't manage it.

☐ Define KPIs/KRIs (false-positive rates, drift, security events, latency and cost).

☐ Set a control-testing calendar and keep evidence in one place with owners.

☐ Use the results to improve prompts, guardrails, and training data—not just to pass audits.

Notes / decisions: _____

9) Incidents & Escalations

When things go sideways, speed and clarity matter.

☐ Prepare playbooks for hallucination, data leakage, model compromise, and harmful content.

☐ Map regulatory thresholds and timelines (Law 25, CPPA/PIPEDA) and who notifies whom.

☐ Pre-approve client/regulator comms; run tabletop exercises twice a year.

☐ Capture lessons learned and track corrective/preventive actions (CAPA).

Notes / decisions: _____

10) People & Training

Tools don't adopt themselves—people do.

☐ Provide role-based training for lawyers, CPAs, developers, and support staff.

☐ Distribute secure-prompting and acceptable-use guidelines; require acknowledgement.

☐ Include deepfake/social-engineering awareness in regular security training.

Notes / decisions: _____

11) Evidence & Auditability

Prove it—or it didn't happen.

☐ Maintain a central evidence register (policies, test results, approvals, PIAs/DPIAs).

☐ Keep versions and traceability from risks → controls → tests → issues → actions.

☐ Structure artefacts by control family to accelerate internal/external reviews.

Notes / decisions: _____

12) Roadmap & Budget

Prioritize ruthlessly and show progress.

☐ Create a heatmap of gaps; identify quick wins (30–60 days), mid-term (90–180), long-term (180+).

☐ Assign owners, budgets, and milestones; publish a simple dashboard.

Notes / decisions: _____

Maturity levels (self-assessment)

Level	What this looks like
0 — Not started	No policy, control, or evidence exists; ownership unclear.
1 — Drafting	Controls or policies drafted; pilots or partial rollout underway.
2 — Implemented	Control deployed and operating; evidence collected routinely.
3 — Measured	KPIs/KRIs monitored; periodic testing, reviews, and tuning occur.
4 — Optimized	Continuous improvement; metrics drive backlog and roadmap changes.

Scoring Worksheet

Domain	Items Complete	Total Items	Score (0–4)	Owner	Due Date
1) Leadership & Accountability					
2) Use-Case Register & Triage					
3) Data & Privacy (Law 25, CPPA/PIPEDA)					
4) Model & System Lifecycle					
5) Security & Resilience					
6) Third-Party & Vendor Risk					
7) Responsible AI & Ethics					
8) Operations & Monitoring					
9) Incidents & Escalations					
10) People & Training					
11) Evidence & Auditability					
12) Roadmap & Budget					