IntelliSync AI Risk Register

Structured Template for Identifying, Logging & Mitigating AI Risks

Prepared by IntelliSync Solutions

This template accompanies the [ORGANIZATION NAME] AI Policy. It provides a structured and detailed way to log, monitor, and mitigate AI-related risks in line with Canadian privacy, human rights, and compliance obligations. It is designed to be flexible enough for organizations of different sizes while maintaining alignment with best practices and Canadian legal frameworks such as PIPEDA, PHIPA, and Québec's Law 25.

Risk Register Table (Sample)

AI-001 ¦ Privacy/Data ¦ Risk of exposing member/client personal information (e.g., SIN, PHI) through prompts in public AI tools ¦ Likelihood: Med, Impact: High, Rating: High ¦ Mitigation: Restrict to enterprise/Canadian data centres; redact inputs; enforce privacy training ¦ Owner: Privacy Officer ¦ Status: Open ¦ Review: 2025-10-01

AI-002 ¦ Bias/DEI ¦ Risk of discriminatory outputs in HR, marketing personalization, or service recommendations ¦ Likelihood: Low, Impact: High, Rating: Med ¦ Mitigation: Prohibit AI for hiring; require bias testing, audits, and human adjudication ¦ Owner: HR Lead ¦ Status: Mitigated ¦ Review: 2025-09-15

AI-003 ¦ Compliance ¦ Non-compliance with Québec Law 25, federal CPPA (Bill C-27), or sectoral rules (finance, healthcare, education) ¦ Likelihood: Med, Impact: Med, Rating: Med ¦ Mitigation: Vendor due diligence; contractual clauses; legal review; regular compliance audits ¦ Owner: AI Officer ¦ Status: Open ¦ Review: 2025-11-01

AI-004 ¦ Security ¦ Malicious prompt injection or adversarial attack that could expose internal systems or proprietary information ¦ Likelihood: Med, Impact: High, Rating: High ¦ Mitigation: Restrict integrations; red-team testing; advanced monitoring; mandatory staff security training ¦ Owner: IT Security ¦ Status: Open ¦ Review: 2025-09-30

Categories of AI Risk

Privacy/Data: Breaches of PIPEDA, PHIPA, Law 25, or other provincial privacy acts; risks of unauthorized data sharing.

Bias/DEI: Biased outputs that may marginalize groups or conflict with Canadian human rights codes.

Compliance: Risks of violating Canadian laws (CPPA, CASL, accessibility laws) or international regulations if tools are cross-border.

Security: Threats from adversarial prompts, data poisoning, model manipulation, or insecure integrations.

Reputational: Risks that damage trust, brand credibility, or community relationships.

Environmental: Resource-intensive AI workloads contributing to climate impacts or excessive cloud costs.

Intellectual Property: Use of copyrighted or trademarked content without consent; challenges to ownership of AI-generated works.

Ethical / Societal: Misinformation, disinformation, erosion of public trust, or impacts on workforce and inclusion.

Likelihood & Impact Scoring (3-point scale)

Likelihood: Low (rare/unlikely), Medium (possible/occasional), High (likely).

Impact: Low (limited), Medium (moderate), High (severe/critical, penalties).

Organizations may adapt to 5-point scale for more granularity.

Risk Rating

Multiply Likelihood x Impact to prioritize mitigation. Example: Med x High = High risk. Colour coding: Green = Low, Yellow = Medium, Red = High.

Lifecycle Management

Intake: Risk assessment before approving AI tool/project.

Monitoring: Quarterly reviews; monitor drift, hallucinations, vendor policy changes.

Incidents: Record events (breach, harmful output, complaint); escalate.

Response: Apply mitigations, communicate, document lessons.

Retirement: Decommission risks, ensure compliant data disposal.

Review Cadence

AI Officer: Quarterly reviews.

AI Governance Committee: Annual review with deep-dive.

Board/Executive: Receive summary dashboards.

Audit/Legal: Periodic independent audits for sensitive use cases.

Companion Practices

Use a heat map dashboard to visualize risks.

Conduct scenario planning for worst-case AI failures.

Align with Canadian ISO/IEC AI Management standards and OECD AI Principles.

Prepared by IntelliSync Solutions

intellisync.io