Risk Management Considerations for Artificial Intelligence (AI) Implementation

Employees are being asked to do more with less, and artificial intelligence is increasingly part of the answer. Today's AI tools are capable of far more than answering routine questions. They can analyze datasets, draft complex documents, summarize case files, assist with research, generate training materials, support policy development, and produce communications across multiple formats.

Integrating AI technology into organizational operations offers benefits, including improved efficiency, cost savings, and enhanced decision-making. However, organizations must identify and manage the potential risks associated with AI adoption to ensure compliance with federal, provincial, and industry-specific regulations. This article outlines key risk management considerations for AI implementation.

The Expanding AI Landscape

The AI landscape has expanded well beyond a single tool. Organizations now encounter a wide range of generative AI platforms, including but not limited to Microsoft Copilot, ChatGPT, Google Gemini, Claude, Perplexity AI, and custom-built chatbots, each with distinct capabilities, data handling practices, and risk profiles. No two tools carry identical risks, and staff may already be using them without formal organizational approval. Rather than evaluating each tool individually, organizations are best served by establishing a clear AI policy that governs how any AI tool may be used, what information may be entered, and who is accountable for outputs.

Data Privacy and Security

AI systems often require large amounts of data to function effectively. Therefore, it is crucial to ensure that the data used by the AI system is stored, processed and transmitted securely to prevent data breaches and unauthorized access. Your organization should implement strong encryption methods, secure data storage solutions and robust access control mechanisms to protect sensitive data. Clearly communicate with staff what information must remain secure and what information can be used with AI.

Legal Issues

Ethical and Legal Compliance

AI systems must operate within the boundaries of applicable ethical and legal frameworks. Before implementation, your organization should develop clear policies and guidelines to ensure that AI systems operate ethically and comply with relevant laws, such as: AI systems must operate within the boundaries of applicable ethical and legal frameworks. Before implementation, your organization should develop clear policies and guidelines to ensure that AI systems operate ethically and comply with relevant laws, such as:

- Data protection regulations
- Anti-discrimination statutes
- Privacy regulations at both the federal and provincial levels, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and applicable provincial legislation such as Ontario's *Freedom of Information and Protection of Privacy Act*

(FIPPA) and *Personal Health Information Protection Act* (PHIPA). The regulatory landscape in this area is actively evolving and is discussed in further detail below.

Potential for Legal Liability

When something goes wrong, the fact that AI generated the output is not a defence. In Moffatt v. Air Canada, the BC Civil Resolution Tribunal rejected the argument that an AI tool operates independently of the organization that deploys it, finding the airline liable for incorrect information its chatbot provided to a customer.[1] While this was a decision of the British Columbia Civil Resolution Tribunal (and not binding precedent), it provides clear guidance on how liability for AI-generated representations may be assessed.

Content an organization produces or publishes, whether written by a person or generated by AI, remains the organization's responsibility. If an employee drafts a communication, publishes information, or makes a decision based on AI output, the organization stands behind that output. Staff must understand what any AI recommendation is based on, what data it analyzed to get there, and whether those sources are credible and applicable to your specific context. The question is not whether AI made the decision. The question is whether your organization can defend it. For a more detailed review of relevant cases please refer to our **Claim Case Study: Artificial Intelligence Case Comparison**.

A Regulatory Conundrum

Artificial intelligence is no longer a future consideration for Canadian organizations. It is already in use across workplaces, and the regulatory environment governing that use is actively evolving. Organizations cannot afford to wait for a single comprehensive law to emerge before taking action. The compliance obligations that exist today are real, and more are on the way.

At the federal level, the proposed *Artificial Intelligence and Data Act* (AIDA), which had been described as Canada's first comprehensive AI legislation, died on the order paper in January 2025 when Parliament was prorogued.[2] As of the date of this revision, Canada has no overarching federal AI law in force. In the interim, the federal government has introduced a Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, which outlines principles including accountability, safety, fairness, transparency, and human oversight.[3] Organizations should be aware that although this code is not legally binding, it may still influence regulatory expectations.

At the provincial level, the regulatory picture is more active, and organizations should pay close attention to developments in their jurisdiction.

For example, in Ontario Bill 194, the Strengthening Cyber Security and Building Trust in the Public Sector Act, this Act applies to public sector entities and creates the authority for the province to regulate how public-sector entities use AI.[4] Ontario has also enacted the Working for Workers Four Act Bill 149, which requires employers using AI to screen or assess job applicants to disclose this practice in job postings.[5]

Other provinces are at earlier stages. British Columbia has published a Policy on the Use of Generative AI and a Digital Code of Practice for public sector employees.[6] The Office of the Information and Privacy Commissioner (OIPC) of Alberta has issued a report which summarizes for the Government of Alberta considerations and recommendations for a legal and policy framework to regulate the use of AI in the province.[7]

For organizations, the practical implication is straightforward. What is voluntary today may inform future mandatory requirements. Organizations that wait for binding legislation before building governance practices will find themselves starting from behind. Those that have already documented their AI use, trained their staff, established clear policies, and assigned accountability will be far better positioned when the rules arrive. Regulators are consistently focused on transparency in the use of AI, preventing discrimination and biased outcomes, preserving human oversight

1 https://www.canlii.org/en/commentary/doc/2025CanLIIDocs1963

2 https://srinstitute.utoronto.ca/news/whats-next-for-aida

3 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

4 https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194

5 https://www.ontario.ca/laws/statute/s24003

6 https://digital.gov.bc.ca/policies-standards/generative-ai-policy/

7 https://oipc.ab.ca/wp-content/uploads/2025/08/AI-Comments-from-the-OIPC-Regarding-Responsible-AI-Governance-in-Alberta-July-15-2025.pdf

over automated decision-making, and accountability for outcomes rather than intent alone. IPE will continue to monitor developments in this area and update guidance as the regulatory landscape evolves. Organizations with questions about their current AI practices or policies are encouraged to reach out.

Transparency

AI systems can make decisions or perform actions that are complex and difficult for humans to comprehend. The resulting lack of transparency and challenges regarding explaining AI-generated answers can cause mistrust, a loss of reputation and could lead to court challenges. Therefore, it's important that organizations aim for AI systems that are transparent in their decision-making process and can provide clear justifications for their actions, should it be necessary to do so. When prompting AI systems for information it is always a good idea to ask for and check sources. AI can and should provide references to justify its response. When prompting AI, staff should request a listing of the sources used and think critically as to whether the sources are relevant for them. That process should be fully documented and retained.

Accountability

Establishing clear lines of accountability is crucial when implementing AI systems. Your organization should identify who is responsible for overseeing the AI system, monitoring its performance and addressing any issues that may arise. This includes assigning responsibility for ensuring compliance with ethical and legal frameworks as well as handling disputes and complaints related to the AI system.

We recommend that organizations have an AI policy. Organizations should establish clear AI policies to guide staff on the appropriate use of AI tools. These policies should outline:

- Approved AI applications and their intended use
- Data privacy and security requirements
- Ethical considerations and responsible AI use
- Employee training and accountability

Having a well-defined AI policy ensures that AI is implemented consistently and ethically across the organization. IPE is available to review AI policies to help organizations mitigate risks and align with best practices.

Training and Education

AI systems can only reach their full potential when users understand how to interact with and use the technology effectively. Staff must be fully trained and understand the capabilities and pitfalls of using AI systems, as well as their responsibilities and potential risks and liabilities of using the technology. Though there is no doubt that effective use of AI will be a total game changer to organizations, it cannot be a "once-and-done." Ongoing vigilance and training are always important, but never more so than with AI. It is essential that staff using these systems keep up to date with news regarding AI.

System Reliability and Robustness

AI systems must be reliable and robust to minimize the risk of errors, failures and unintended consequences. Your organization should thoroughly test and validate AI systems before implementation and continuously monitor their performance to identify and address any issues that may arise. This includes conducting regular system maintenance and updates to ensure optimal performance.

Vendor Selection and Management

When selecting AI technology vendors, your organization should carefully evaluate their offerings, track record, and commitment to ethical and legal compliance. Keep in mind there are different vendors for different tasks. Some specialize in specific tasks such as copywriting, whereas some vendors have more general capabilities. Be sure to research which AI system will be able to best provide for your organization's needs.

Data residency is an increasingly important consideration. Many of the most commonly used AI platforms are operated by American corporations and process data on servers located outside of Canada.

IPE is available to review your vendor agreements to ensure your best interests are protected.

Public Perception and Communication

The public's perception of AI technology can have a significant impact on your organization's reputation and operations. It is essential to communicate openly and transparently with the public about your organization's use of AI technology, its benefits and the measures taken to address potential risks and concerns.

Socio-Ethical and Environmental Considerations

AI and machine learning systems require significant resources to function, including vast amounts of computational power, electricity, and even water for cooling data centers. Organizations must consider the environmental impact of AI adoption. Additionally, ethical considerations extend beyond data privacy to include the societal effects of AI, such as job displacement and algorithmic biases that could reinforce existing inequalities. Addressing these issues requires a balanced approach that prioritizes responsible AI development and deployment.

Understanding Limitations

AI systems, while powerful and versatile, have limitations that must be understood and managed. These limitations can include biases in training data, difficulty in understanding context, sensitivity to data input changes and potential for "overfitting" which can occur when the AI makes conclusions that will not have relevance to your specific organization. Your staff should be aware of these limitations and develop strategies to mitigate potential risks from these limitations. Again, training your staff to know what to watch for and mitigate against is integral to AI integration for effective use.

Use of AI holds much promise. Many organizations will certainly benefit from creating more efficiencies and saving staff costs. AI, however, is a tool, it is not a panacea or cure against critical thought. By addressing these risk management considerations and remembering that these considerations can and will change, your organization can maximize the benefits of AI technology while minimizing potential risks and challenges.

As of May 2026, at the time of writing his article, the information provided represents our understanding of Artificial Intelligence (AI) technology. However, please note that AI is a rapidly evolving field, and new advancements and information may emerge, potentially altering our current knowledge. Readers are encouraged to stay informed about the latest developments and consult reliable sources for the most up-to-date information on AI.

intact public entities