

IAPP Cross-Canada KnowledgeNet Event

Beyond the Chaos: Practical
Application of AI Governance

Data Privacy Day, January 28, 2026

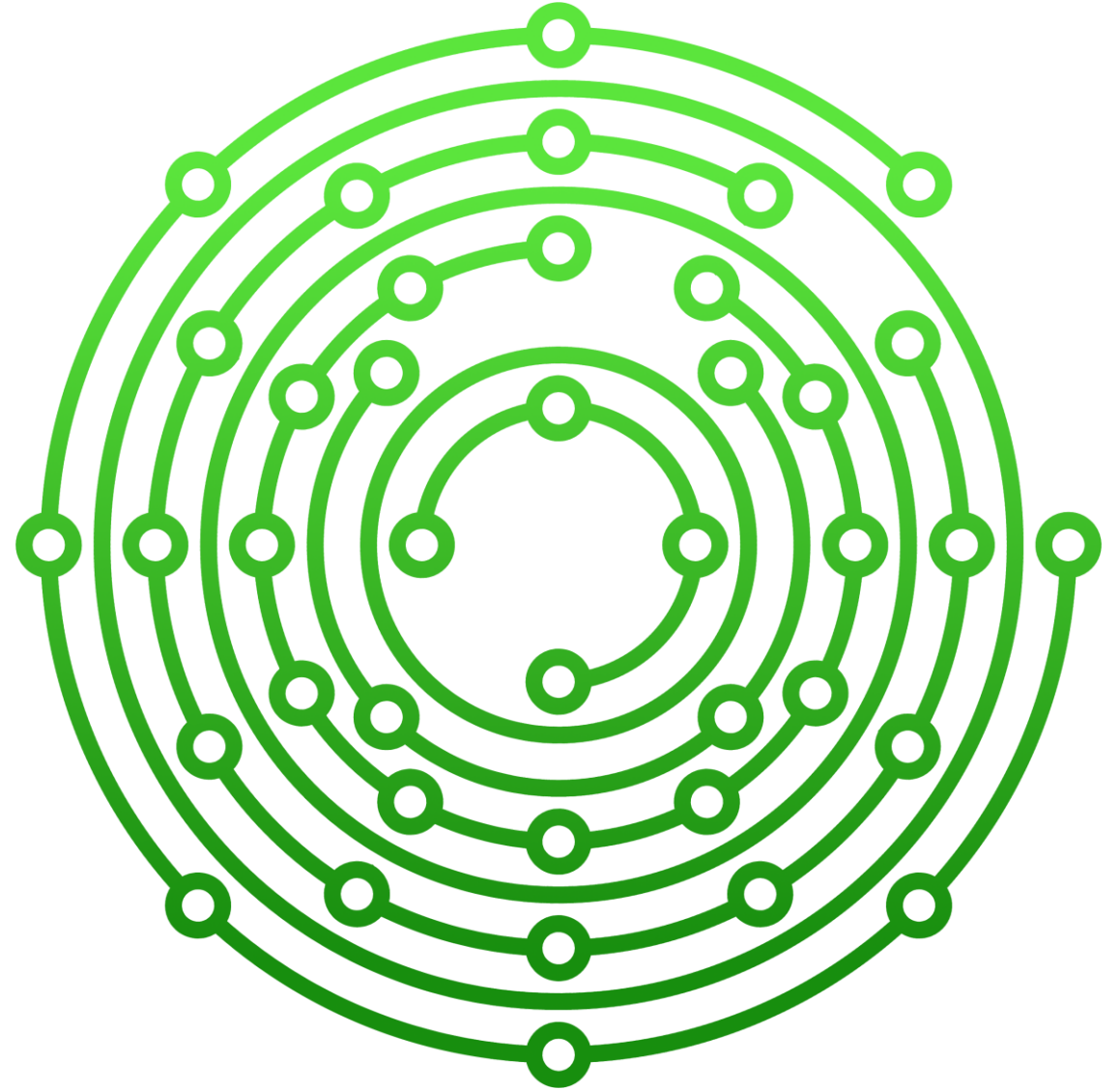


Table of Contents



Introduction



Executive Summary



Poll Question Results



Six Pillars of Effective AI Governance



Appendix

Introduction



On January 28, 2026, privacy professionals in 10 cities across Canada came together to explore the topic of AI governance. The session was intended to foster conversation with a view to helping organizations consider how best to reap the benefits of AI without compounding the risks.

Participants heard from Privacy Commissioners in Newfoundland and Labrador and BC, along with a panel of experts who conveyed the importance and practical realities of AI governance today. Attendees in each city then probed into specific aspects of AI governance to further uncover the challenges and best practices for organizations to follow. This report serves as a summary of the conversations from the day.

During the event, it was highlighted that responsible AI governance must be grounded in strong privacy principles such as data minimization, accountability, and transparency. AI systems pose critical risks including opacity, loss of individual autonomy, societal disruption, job displacement, and impacts on education, which contribute to public concerns and discomfort about AI-driven decisions.

Importance of maintaining individual control over personal data to foster trust and protect human dignity is essential. Proactive risk management through early privacy impact assessments, ongoing policy updates, and public engagement will all aid in responsible use of personal information in AI systems. Ultimately, the need for transparent, ethical, and human-centered AI governance that evolves with technology will be a cornerstone to prioritizing trust, accountability, and stakeholder rights.

Executive Summary



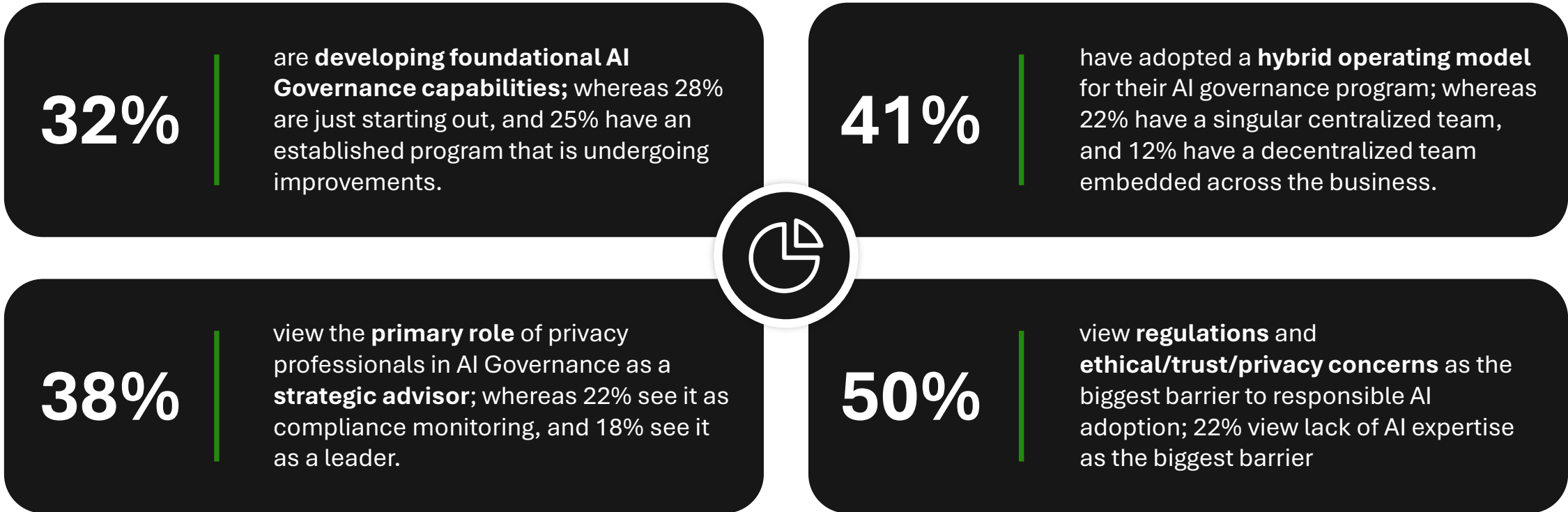
As organizations adopt artificial intelligence (AI) technologies, the focus should be on governing AI responsibly rather than suppressing its potential. However, many organizations face challenges in AI governance due to uncertainty about where to begin. The key objective is to take proactive steps. Starting somewhere is critical, even if the initial approach only provides incremental change to the current state. Implementing a foundation will help you learn about the organization's use of AI that can serve as a basis for building a more comprehensive program.

- **The AI landscape is dynamic, with rapid advancements in technology and evolving regulatory requirements.** Organizations must establish flexible governance programs that can adapt to these changes. Both public and private sector tools and frameworks are available to support the development of governance structures, and leveraging these resources can provide valuable guidance for organizations at any stage of their AI journey.
- **Canada is not without legal oversight on AI.** Existing legal regimes including privacy, civil liability, employment, and copyright laws, remain applicable and relevant to AI implementation. Organizations should recognize that these laws provide a foundational layer of governance, even as new AI-specific regulations are being considered.
- **Effective AI governance will require strong cross-collaboration with several teams.** The teams involved will vary depending on the size and nature of your organization, but will likely include groups from technology, risk and compliance, legal, and product development. Each area will have a role to play in building a governance structure that aligns to the use cases for which your organization may intend to leverage AI. Seeking input from all areas and ensuring responsibilities are clearly defined will be essential to appropriate oversight and risk mitigation as your organization embarks on its AI journey.
- **An effective method for establishing a foundation is for organizations to align and embed AI governance into existing frameworks.** This approach can help to simplify processes and reduce complexities of oversight. Identify which assessments may be best suited to incorporating aspects of AI governance and note gaps which may require establishment of new processes to ensure all key areas of AI risk are considered.
- **Change management and training are essential components for successfully deploying governance.** Creating a common language for your organization around AI and developing educational materials to ensure all employees have a base understanding of the risks with this technology will foster a culture of transparency and trust. Considering role-specific training will further enhance the capabilities of those who may be actively involved in the deployment of AI to proactively mitigate the detrimental effects and ensure monitoring is in place to track when issues arise.
- **AI can serve to drive benefits for society and create innovative new solutions** to pressing problems in today's world. The key will be to ensure appropriate oversight is placed around this technology and the data that powers it to effectively drive these benefits without creating subsequent harms to individuals. The best approach is to start small, learn, create feedback loops, and adapt your governance structure as internal and external factors evolve.

Poll Question Results

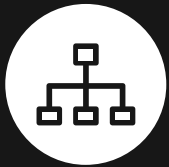
Several questions were posed to attendees to gain insight into the current state of AI governance in organizations across Canada. Results from 113 respondents indicated that many are still in the early stages of establishing governance programs and that there are key concerns which need to be addressed to effectively advance governance practices.

Participants reported that at their organization...

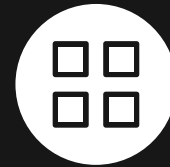


Six Pillars of Effective AI Governance

Effective AI governance requires a risk-based, integrated framework, clear roles and responsibilities, practical assessment tools, robust metrics and monitoring, ongoing change management and training, and strong alignment with existing organizational programs. Success depends on building transparency, trust, and appropriate oversight to monitor AI practices throughout the lifecycle. Establishing your program with an ability to readily adapt to the evolving technological and regulatory landscape will be imperative.



1. Determination of AI governance framework



4. Alignment for AI programs/assessments and existing privacy programs



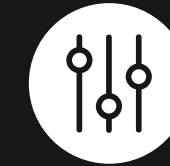
2. Establishing roles and responsibilities for AI governance



5. Change management, training and education



3. Identifying the right assessment tools and processes to implement



6. Metrics and monitoring to determine how the program is performing

1. Determination of AI Governance Framework

Establishing a framework for your AI governance program is the first key step towards responsible and ethical use of AI. Selecting and adapting a framework that matches your organization’s size, industry, and business objectives will allow you to establish a clear, defensible foundation to leverage AI in a risk-focused manner.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
• Risk-based and principle-driven governance rather than one-size-fits-all controls • Integration over reinvention: leverage existing frameworks such as ISO 42001 and NIST AI RMF • Establish clear governance structures with executive-level support and cross-functional collaboration • Focus on practical risk management, transparency, and trust-building	• Look to existing laws and regulations for guidance – even if you aren’t required to adhere to them • Define clear policies, acceptable use cases, no-go zones, and tiered risk categories • Embed AI governance into existing committees and processes, avoiding parallel structures • Ensure frameworks are realistic, resource-friendly, and adaptable to organizational maturity	• Decentralized oversight and unclear ownership • Lack of common understanding of AI and associated risks within the organization • Consideration for managing vendor management and third-party AI visibility within the governance structure • Resource constraints and organizational resistance to change	• Start small and be prepared to adjust as the technology and regulations evolve • Have regular monitoring and review of the governance structure to identify improvements • Strong alignment between privacy, risk, and AI decision-making, with clear accountability and ownership • Seek to improve transparency and trust with all stakeholders

KEY TAKEAWAY: Effective AI governance is achieved by adapting what already works, applying it consistently to AI risks, and grounding decisions in privacy, transparency, and accountability.

2. Establishing Roles and Responsibilities for AI Governance

Clearly defining roles and responsibilities within the organization for managing AI through the lifecycle is an essential component for an effective program. Identifying accountability creates clear expectations across all functions where certain tasks will be completed and the parties who need to be involved in making decisions for AI management.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
• Clear ownership for AI governance, often led by IT with input from privacy, legal, compliance, and business units • Multidisciplinary teams with defined roles and accountability • Formal governance structures such as Centers of Excellence or governance committees can support importance of proper governance • Document and communicate responsibilities for all parties involved and adjust to meet changing requirements	• Clarify ownership and accountability across all identified parties for your organization • Assign distinct roles: business owner, technical owner, risk owner • Define reporting structures and approval workflows • Ensure Board and Executive-level oversight • Involve end users in deployment and evaluation, combining bottom-up and top-down approaches • Address vendor and third-party responsibilities, including documented risk acceptance and contract terms	• Unclear or fragmented ownership across functions • Gaps between technical, legal, and operational perspectives • Handling vendor accountability and third-party risk management can create additional complexity • Difficulty sustaining oversight as organizations and AI use cases evolve	• Clearly defined and understood AI roles across the organization • Active Executive and Board engagement • Coordinated decision-making across functions and clear escalation paths when required • Documented accountability for internal and third-party AI systems • Ongoing review and adjustment of responsibilities as AI use evolves • Establish clear responsibilities for managing ‘human-in-the-loop’ processes to readily identify and correct issues

KEY TAKEAWAY: AI governance succeeds when ownership is explicit, shared across disciplines, and supported by executive oversight, with responsibilities that are documented, communicated, and regularly reviewed.

3. Identifying the Right Assessment Tools and Processes to Implement

To effectively manage AI, several aspects should be assessed to identify potential risks. Processes and tools for these assessments should be scaled to fit your organization’s structure and use cases. Careful consideration will need to be given as to how identifying AI risks will integrate with existing structures across the various departments which will play a role in the overall management of AI.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
- Use impact-based assessments aligned with organizational size and risk - Address data minimization, ethical considerations, and regulatory compliance - Treat third-party and vendor AI as a core risk area - Ensure assessments are ongoing, not one-time exercises	- Determine appropriate assessment tools to properly identify risks associated with AI deployment, such as privacy impact assessments (PIAs), algorithmic impact assessments (AIAs), information management assessments, security assessments - Track all AI technology in use across the organization including ‘shadow AI’ (e.g. unauthorized AI tools) - Use surveys and intake forms to capture AI use cases, data types and dependencies to understand how the organization is or is intending to use AI - Conduct line-of-business walkthroughs to identify gaps, risks and opportunities for enhancing AI governance structure - Link assessments to real-world impacts and rights-based principles to make them meaningful and relatable for business owners - Update data sources and workflows that are powering AI solutions to manage changes over time - Regularly assess and monitor human-in-the-loop controls - Maintain documentation, audit trails, and reporting requirements	- Lack of visibility into AI tools already in use - Inconsistent assessment approaches across business units - Limited oversight of vendor and third-party AI practices - Treating assessments as static compliance tasks rather than continuous risk management	- A complete and current inventory of AI tools - Consistent use of assessment tools within the organization - Clear documentation and auditability - Regular reassessment tied to changes in data, vendors, or use cases - Tiered, risk-based assessment framework that considers materiality and overall impact of initiatives

KEY TAKEAWAY: Effective AI assessment is continuous, practical, and impact-focused—combining strong intake processes, fit-for-purpose tools, and real operational follow-through.

4. Alignment for AI Programs/Assessments and Existing Privacy Programs

Existing privacy programs hold several parallels to effective AI governance. Leveraging the knowledge and experience from establishing privacy within your organization can serve as a guide to aligning AI within the programs or assessments you currently use.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
- AI governance should be embedded early, not bolted on later Leverage existing privacy laws and sectoral regulations to guide AI assessments and compliance - Ensure consistent data management practices across AI and privacy programs (e.g., data minimization, data sovereignty) - Promote cross-functional coordination to avoid siloed governance and fragmented oversight	- Integrate AI governance with existing privacy, data, and risk management frameworks - Consider the full AI lifecycle within your governance structure - Align AI policies with regulatory requirements, organizational values, and professional standards - Ensure transparency, stakeholder rights (e.g., consent, access, appeal), and ethical controls - Incorporate AI into existing infrastructure: policies, tools, processes, and compliance/reporting mechanisms	- Siloed AI initiatives disconnected from privacy and risk programs - Inconsistent data practices between AI and non-AI systems - Lack of coordination across functions involved in AI decisions - Treating AI governance as a separate compliance exercise rather than an extension of existing programs	- AI governance fully embedded within existing privacy and risk programs - Consistent application of data protection and ethical principles across all AI use cases - Unified oversight through coordinated cross-functional teams - Clear linkage between AI decisions, regulatory obligations, and organizational values - Reduced duplication and more efficient governance processes

KEY TAKEAWAY: AI governance is most effective when it is **not separate**, but **deeply aligned with existing privacy, data, and risk programs**, ensuring consistency, efficiency, and trust across the organization.

5. Change Management, Training and Education

Communicating the components of your AI governance program to the organization is a critical component to success. Identifying multiple channels by which to educate and inform employees about responsible use of AI, the structure of how AI is governed in the organization and the potential risks of misuse of the technology all play a role in minimizing the potential risks.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
• Ongoing AI and digital literacy for all staff • Role-based training aligned to responsibilities and system usage • Proactive change management, not reactive enablement • Inclusive approaches that address cultural hesitancy and digital divides	• Develop an organization-wide training and communications strategy • Provide tailored, continuous training reflecting roles, backgrounds, and AI exposure • Build AI literacy including risk, privacy, ethical decision-making, and incident escalation • Use diverse formats: micro-learning, videos, infographics, newsletters, dashboards, intranet • Engage stakeholders early to foster buy-in and reduce resistance • Involve change managers and adult educators in planning and delivery • Maintain recurring refresher training and update content as requirements evolve	• One-size-fits-all training that ignores role differences • Cultural resistance and fear of AI-driven change • Gaps in awareness of privacy, risk, and ethical implications • Training treated as a one-off activity rather than an ongoing program • Diversity of understanding and comfort with AI technologies among employees	• Workforce understands why AI is used and how risks are managed • Training aligned to real workflows and decision-making • Clear definitions of key terms to enable consistency in communication • Sustained engagement through refreshed, relevant learning • Increased confidence and responsible use of AI across the organization

KEY TAKEAWAY: Successful AI adoption depends as much on people and culture as on technology—effective change management and tailored education are essential to responsible governance.

6. Metrics and Monitoring to Determine how the Program is Performing

Establishing metrics, Key Performance Indicators (KPIs) and other forms of measuring the effectiveness of your AI initiatives will help to track these over time and assist in identifying when outcomes are veering outside the organization’s risk appetite.

FOUNDATIONAL PRINCIPLES	HOW TO IMPLEMENT	COMMON CHALLENGES	WHAT “GOOD” LOOKS LIKE
- Metrics must go beyond financial indicators to include risk, compliance, and trust - Monitoring should be continuous, not episodic - Oversight should be proportionate and actionable, avoiding over-governance Align metrics with your organization’s business objectives	- Define KPIs that track important aspects of AI governance for your organization – including regulatory compliance, AI adoption, ethical outcomes and benefit realization - Monitor AI to track use of AI by employees – both approved and non-approved tools - Record and report incidents to rectify issues and utilize the outcomes to inform changes to your program or use of AI - Review governance program regularly – every 6 to 12 months – and establish a regular reporting cadence to the Board, Executives and relevant governance committees	- Over-reliance on financial or adoption metrics - Limited visibility into employee and vendor AI use - Monitoring that generates data but not decisions - Governance controls that are not properly risk-aligned	- KPIs clearly linked to risk mitigation and responsible outcomes - Continuous visibility into AI tools, usage, and vendors - Metrics actively used to improve governance and strategy - Clear, regular reporting to leadership and stakeholders - Monitoring that supports innovation while maintaining trust

KEY TAKEAWAY: Metrics and monitoring are effective when they **inform decisions, demonstrate responsibility, and evolve with AI risk**, rather than serving as static compliance reporting.

Appendix



Other Insights



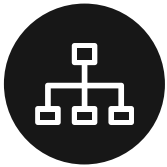
Full Poll Results



Additional Resources

Other Insights that may Impact your AI Governance Strategy

Topics beyond the six key areas came up through the panel discussion and ensuing chapter discussions on additional aspects that can impact AI governance. These provide further context that can be considered when developing your AI strategy and influence how your organization might establish appropriate oversight controls to ensure the technology is deployed responsibly.



Data Sovereignty & Cross-Border Data Flows

- Data sovereignty is a significant and complex issue, with Canada facing challenges due to small market power, dependence on global cloud vendors, and cross-border data flows.
- Data sovereignty is not solely a technical issue but a broader social project, with governments playing a role in defining “safe” data practices.
- The European Health Data Space (EHDS) regulation was highlighted as a template for guardrails, aggregated health data use, interoperability, and secure secondary use environments.
- Ongoing European work on guidelines related to security and safety was noted as relevant for Canadian organizations.
- Key considerations include where data is stored, where vendors are located, and how data moves across borders.



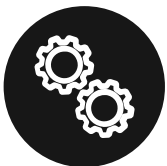
Vendor Management & Power Imbalance

- Power imbalance with major vendors is profound, making negotiation and transparency challenging.
- Smaller AI vendors in Canada may offer better insight into system design and data practices, providing opportunities for more collaborative governance.
- Organizations have limited ability to push vendors to change their AI practices; the Canadian market is often perceived as too small to significantly influence multi-national AI vendors.



Transparency & Trust

- Transparency regarding AI models and the data used to train and operate them is essential for trustworthy AI governance.
- Understanding model limitations, the risks they introduce, and mitigation strategies is critical for responsible AI use.

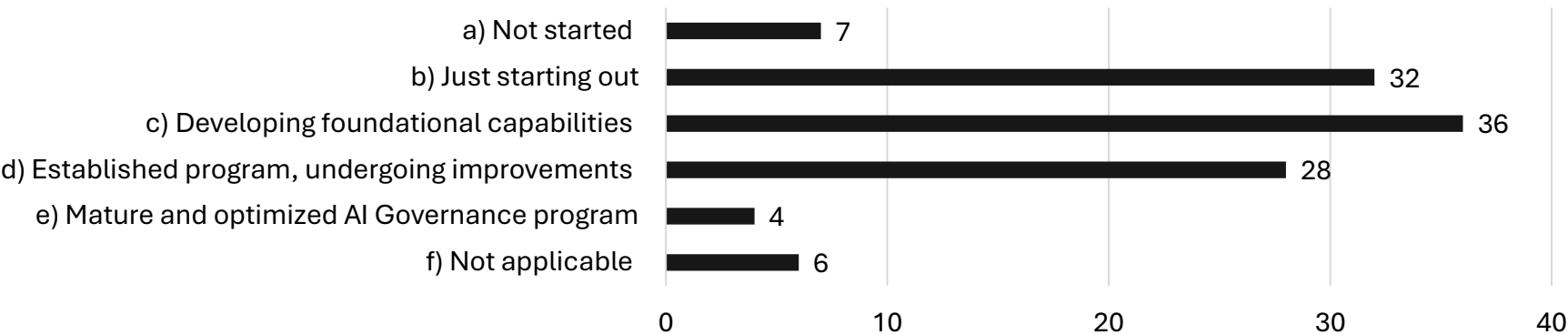


Regulatory & International Alignment

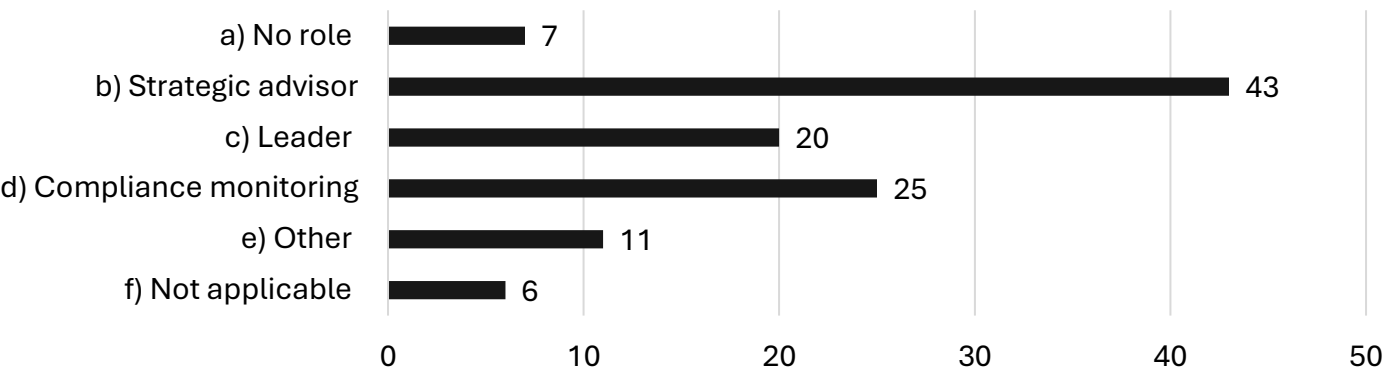
- Governments and organizations should not wait for new AI legislation but proceed with best available guidance, treating AI like other business risks and updating continuously.
- The European Health Data Space regulation was mentioned as a model for other countries seeking access to data governed by this framework.
- Address data sovereignty and cross-border data flows; consider international models (GDPR, EU AI Act) to guide your organization’s AI governance practices.

Full Poll Results (1 of 2)

Q1: Where is your organization on its AI Governance journey?



Q2: What is the primary role of Privacy professionals in AI Governance in your organization?

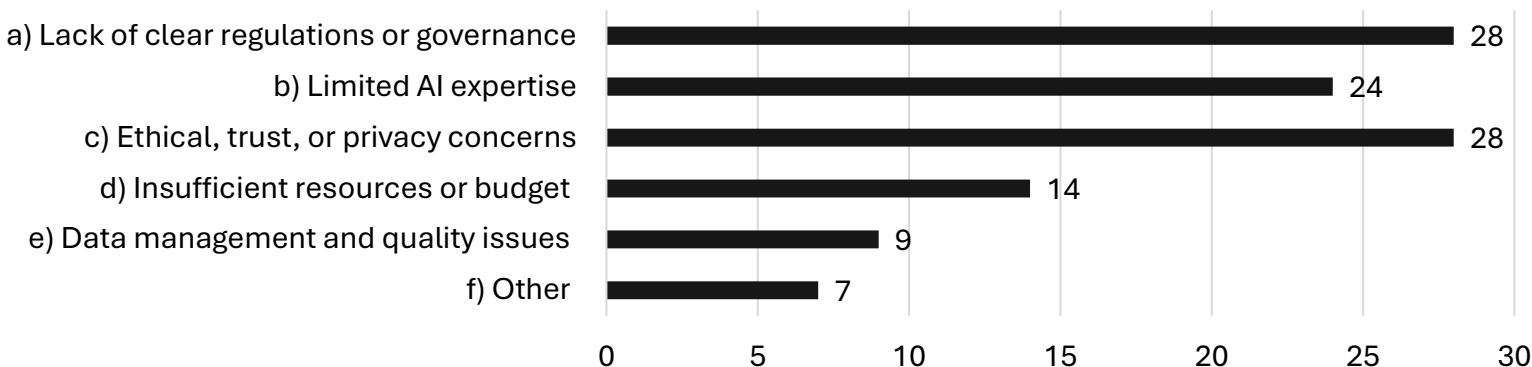


Full Poll Results (2 of 2)

Q3: What type of AI Governance Operating Model does your organization have?



Q4: What is the biggest barrier to responsible AI adoption at your organization?

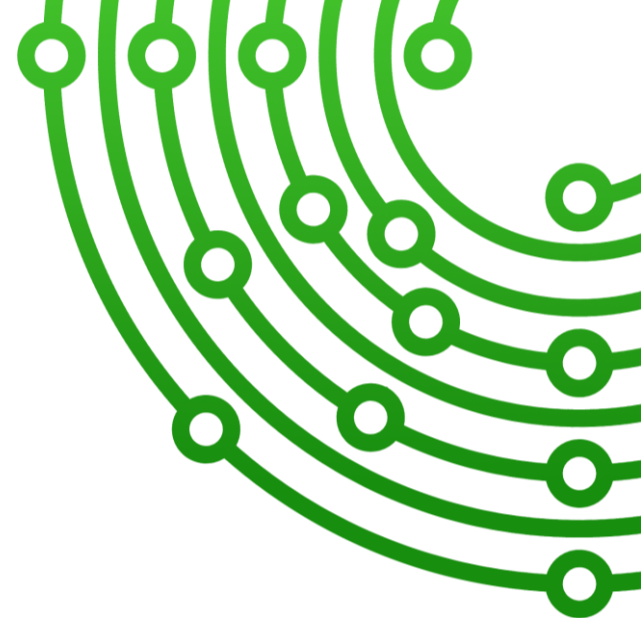


Additional Resources

Many resources are available that can help guide your AI governance journey. While these span both public and private sector, they can serve to inform your implementation and be adapted to meet your organization's specific needs.

- **NIST AI Risk Management Framework:** <https://www.nist.gov/itl/ai-risk-management-framework>
- **ISO/IEC 42001:** <https://www.iso.org/standard/42001>
- **Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems:** <https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems>
- **Guide on Departmental AI Responsibilities – Government of Canada:** <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/guide-departmental-ai-responsibilities.html>
- **Algorithmic Impact Assessment tool – Government of Canada:** <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>
- **Implementation guide for managers of Artificial intelligence systems:** <https://ised-isde.canada.ca/site/ised/en/implementation-guide-managers-artificial-intelligence-systems>
- **EU AI Act – Article 5 Prohibited AI Practices:** <https://artificialintelligenceact.eu/article/5/>
- **EU AI Act – Article 6 Classification Rules for High-Risk AI Systems:** <https://artificialintelligenceact.eu/article/6/>





This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte Canada

At Deloitte, our Purpose is to make an impact that matters. We exist to inspire and help our people, organizations, communities, and countries to thrive. Our work underpins a prosperous society where people can find meaning and opportunity. It builds consumer and business confidence, empowers organizations to find imaginative ways of deploying capital, enables fair, trusted, and functioning social and economic institutions, and allows our friends, families, and communities to enjoy the quality of life that comes with a sustainable future. And as the largest Canadian-owned and operated professional services firm in our country, we are proud to work alongside our clients to make a positive impact for all Canadians.

Deloitte provides industry-leading consulting, audit and assurance, tax, advisory and managed services to nearly 90% of the Fortune Global 500® and thousands of private companies. We bring together world-class capabilities, insights, and services to address clients' most complex business challenges.

Deloitte Inc., an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

To learn more about Deloitte Canada, please connect with us on [LinkedIn](#), [X](#), [Instagram](#), or [Facebook](#).

© 2026 Deloitte Inc. and affiliated entities.

