AI Security

Governance, Risk and Compliance (CGI AI GRC) offering

Enabling secure AI adoption for your organization

Canada

CGI

Contents

Executive summary

When it comes to artificial intelligence (AI), there is no single path. Not only do organizational needs differ and evolve over time, but the technology itself is also evolving rapidly and becoming increasingly integrated into third-party platforms.

Technological innovation has rarely come without a security trade-off, with risk often treated as an acceptable by-product of competitive progress. While there is no denying the growing role AI plays in data-driven decision-making and operational efficiency, it is also exposing a deepening divide between AI readiness and data security. This is evident in the fact that over 75% of organizations report AI-related security breaches, while only about 30% have adopted effective data classification practices*.

A majority of organizations are not adequately prepared to secure their AI-driven initiatives, lacking both a cohesive cybersecurity strategy and the necessary technical capabilities to defend against AI-augmented threats. The advent of agentic AI presents an even greater risk: autonomous AI agents do not simply process data; they make decisions, trigger actions and operate across systems with minimal human oversight. Data misuse, algorithmic bias, uncontrolled model drift and regulatory violations are no longer hypothetical risks—they are active fault lines running beneath every AI deployment.

Organizations that embed Governance, Risk and Compliance (GRC) into their AI strategy are not just managing today's risks—they are laying the foundation for the demands of tomorrow's AI landscape. As regulatory frameworks such as the EU AI Act, ISO/IEC 42001:2023 and local government guidelines (e.g., Bill 194 in Ontario) are developed and introduced, organizations are under increasing pressure to demonstrate that their AI initiatives are implemented not only effectively but also securely, ethically and with strong governance.

CGI supports organizations in this effort by providing capabilities in regulatory alignment, threat modeling, risk assessment, internal auditing, and workforce awareness, enabling them to confidently scale AI adoption while maintaining trust, transparency and control, with a clear focus on ROI.

With five decades of deep expertise in cybersecurity, risk management, and regulatory advisory in Canada and globally, CGI helps transform AI from a potential liability into a secure and strategic capability for your organization.

Security Magazine, 3 Top Cybersecurity Trends from 2025, November 2025

AI Governance, Risk and Compliance (AI GRC) by CGI

CGI's AI GRC offering combines six services to help CISOs, CDAOs and AI leaders build the structures, policies and processes needed to govern AI responsibly end to end, enabling trusted, scalable AI adoption while aligning with each organization's sector-specific regulatory requirements.

AI Regulatory & Compliance Consultation

Expert guidance for leadership on understanding, mapping and proactively managing the compliance obligations associated with AI initiatives

Capabilities

What's included:

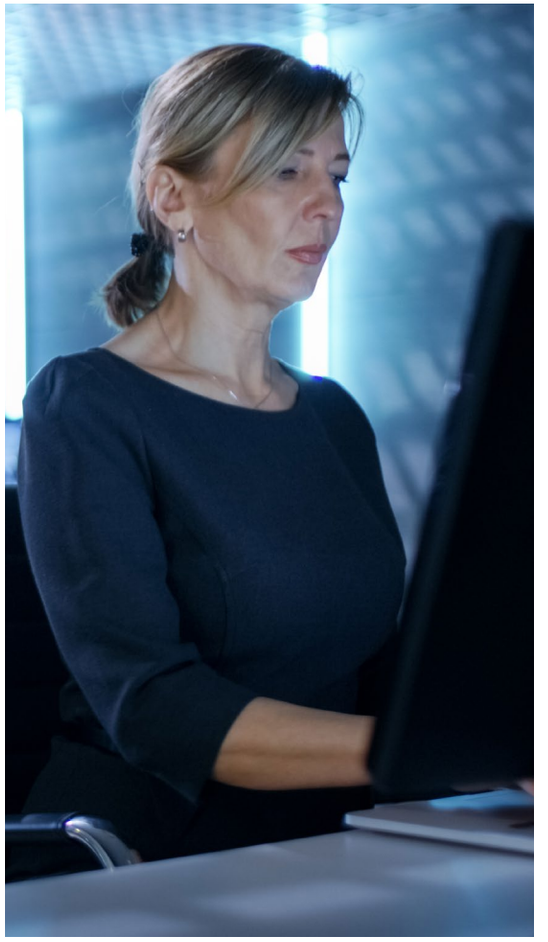
- Regulatory mapping and gap analysis
- Development of an AI-specific compliance framework
- Alignment with privacy and data protection regulations
- Monitoring of AI legislation and horizon scanning
- Client-specific impact analysis
- Engagement and representation support

Key benefits

- Reduced regulatory and legal exposure
- Improved compliance readiness
- Clear interpretation of evolving AI legislation
- Stronger, more defensible AI governance posture

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response



AI Risk Management Framework Development

A comprehensive, consolidated view of AI risk, combining rigorous assessment methodologies with proprietary tools purpose-built for AI environments

Capabilities

What's included:

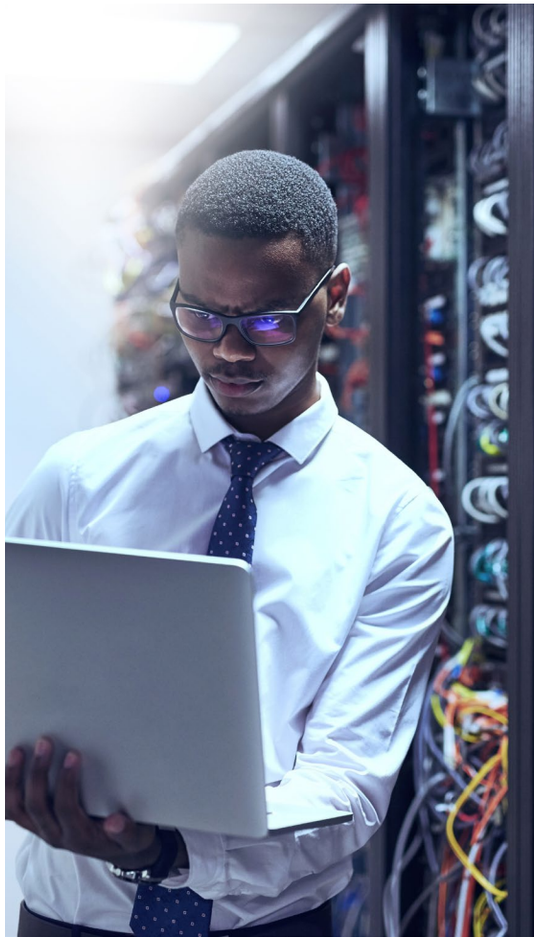
- Adoption and tailoring of existing frameworks
- Development of custom frameworks
- Framework integration
- Ongoing review and updates
- Custom AI threat modeling

Key benefits

- Comprehensive identification and mitigation of AI risks
- Integration with enterprise cybersecurity frameworks
- Continuous improvement of AI risk management processes
- Enhanced resilience against emerging AI threats

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response



AI Threat, Risk and Privacy Impact Assessments

The development of a structured approach to identifying, mitigating and managing AI risk, combining industry-leading frameworks with custom threat modeling methodologies tailored to your environment

Capabilities

What's included:

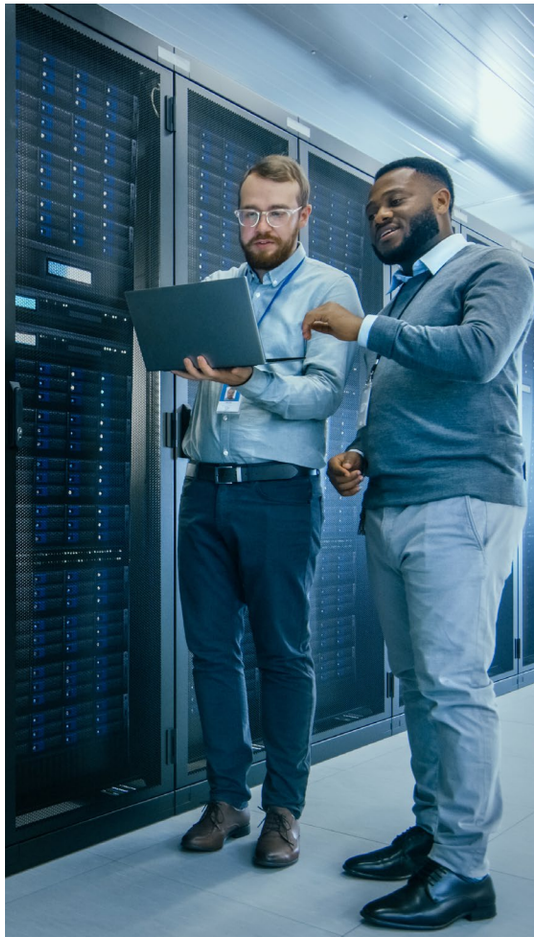
- AI threat and risk assessment (AI TRA)
- AI privacy impact assessment (AI PIA)
- Proprietary AI assessment tools

Key benefits

- Clear risk ratings and remediation guidance
- Identification of vulnerabilities in AI architecture
- Improved data protection and privacy compliance
- Actionable insights for security teams

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response



AI Management System (AIMS) Internal Auditing – ISO/IEC 42001

Expert-led internal auditing of your AI systems, with rigorous assessment of the policies, processes, controls and governance structures required to meet the ISO/IEC 42001:2023 standard

Capabilities

What's included:

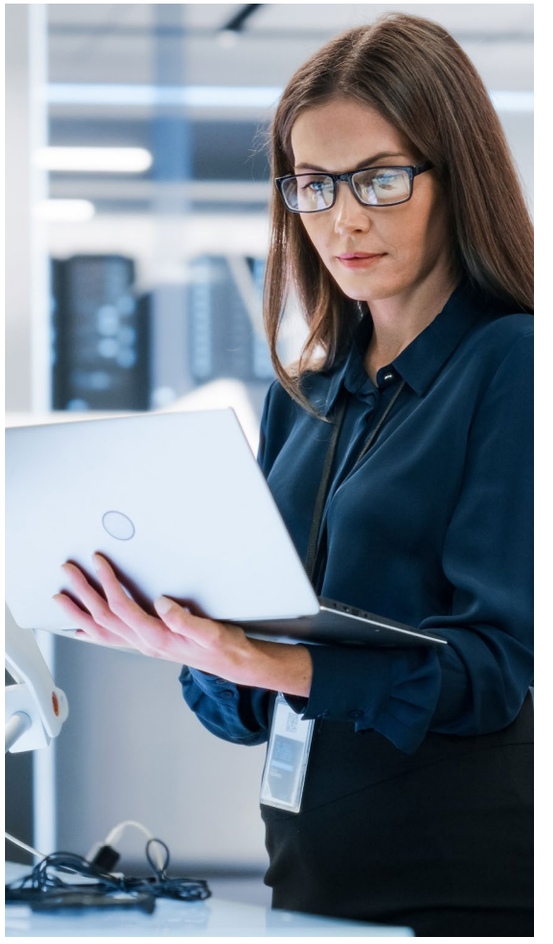
- ISO/IEC 42001 readiness assessment
- Internal AIMS audit
- Policy and control review
- Evaluation of AI objectives and performance
- Corrective action and continual improvement support

Key benefits

- Improved readiness for ISO/IEC 42001 certification
- Clear remediation roadmap for compliance gaps
- Strengthened governance and accountability
- Demonstrated commitment to responsible AI

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response



About ISO/IEC 42001:2023

According to the International Organization for Standardization (ISO), "ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining and continually improving an Artificial Intelligence Management System (AIMS) within organizations. The standard is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems."

ISO also defines an AIMS as "a set of interrelated or interacting elements of an organization intended to establish policies and objectives, as well as processes to achieve those objectives, in relation to the responsible development, provision or use of AI systems."

ISO has developed a number of standards to help organizations mitigate the risks and maximize the benefits of AI, including ISO/IEC 23894. The key difference between ISO/IEC 23894 and ISO/IEC 42001 lies in their scope. While ISO/IEC 23894 adapts general risk management standards (ISO 38001-2018) for AI, ISO/IEC 42001 focuses on how organizations design, adopt and document internal operating procedures to manage their AI systems.

What are the primary benefits of implementing ISO/IEC 42001?

- International recognition: ISO/IEC 42001 is an internationally recognized standard; particularly valuable for multinational organizations.
- Responsible AI: Supports the ethical and responsible use of AI.
- Reputation management: Strengthens trust in AI applications.
- AI governance: Helps ensure compliance with legal and regulatory requirements.
- Practical guidance: Provides a structured approach for managing AI-specific risks effectively.
- Opportunity identification: Encourages innovation within a structured framework.

Source: ISO/IEC 42001:2023 – AI management systems

What recommendations does Annex A of the ISO/IEC 42001 provide for organizations?

Annex A provides a list of 38 controls under the following 9 domains.

ID	Generative AI	Agentic AI
A.2	Policies Related to AI	Requirements for documenting an AI policy and ensuring it aligns with other corporate policies (e.g., privacy, security).
A.3	Internal Organization	Definition of roles and responsibilities (e.g., AI Ethics Officer) and establishment of processes for reporting AI-related concerns.
A.4	Resources for AI Systems	Documentation of technical, data, human and computing resources used at each stage of the lifecycle.
A.5	Assessing AI Impacts	Mandatory processes for evaluating the impact of AI on individuals, society and human rights (impact assessments).
A.6	AI System Life Cycle	Controls covering the full lifecycle: design, development, verification, validation, deployment and decommissioning.
A.7	Data for AI Systems	Standards for data quality, acquisition, provenance (lineage) and preparation/cleaning.
A.8	Information for Parties	Requirements for transparency, including informing users and regulators about how the AI system works and its limitations.
A.9	Use of AI Systems	Rules for the responsible operation of AI, including human oversight and the prevention of "scope creep."
A.10	Third-Party Relationships	Controls for managing risks associated with external models (e.g., OpenAI, Gemini) and third-party AI service providers.

Connect with our team to explore how we can help you implement these recommendations.

AI Security Advisory & Governance

The establishment of strong governance structures and responsible AI practices across your organization.

Capabilities

What's included:

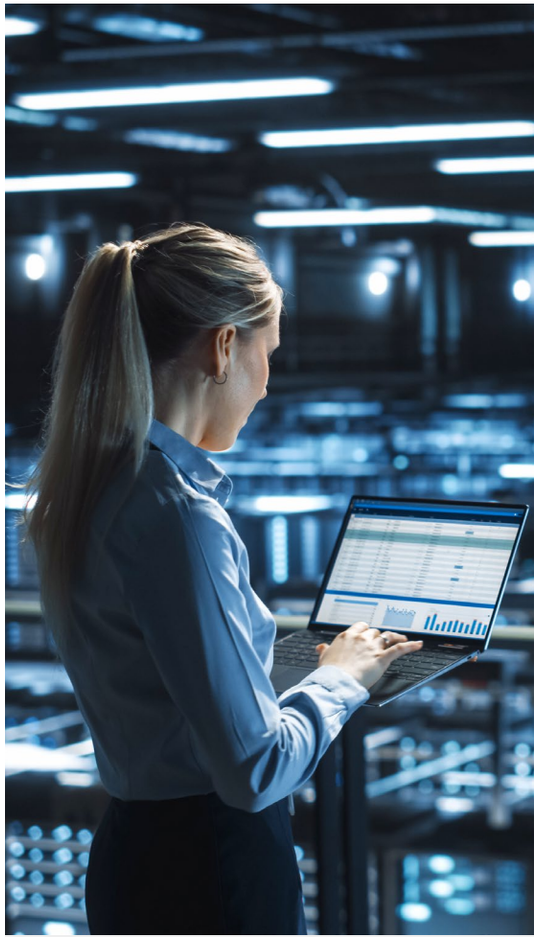
- AI governance maturity assessment
- Governance framework design
- AI policy development
- AI readiness and responsible use advisory

Key benefits

- Clear governance structures and accountability
- Responsible and ethical AI deployment
- Alignment between AI initiatives and business objectives
- Increased confidence in AI adoption

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response



AI Security Awareness Training

Role-based training programs designed to help your teams engage with AI securely, responsibly and ethically—from the front line to the boardroom.

Capabilities

What's included:

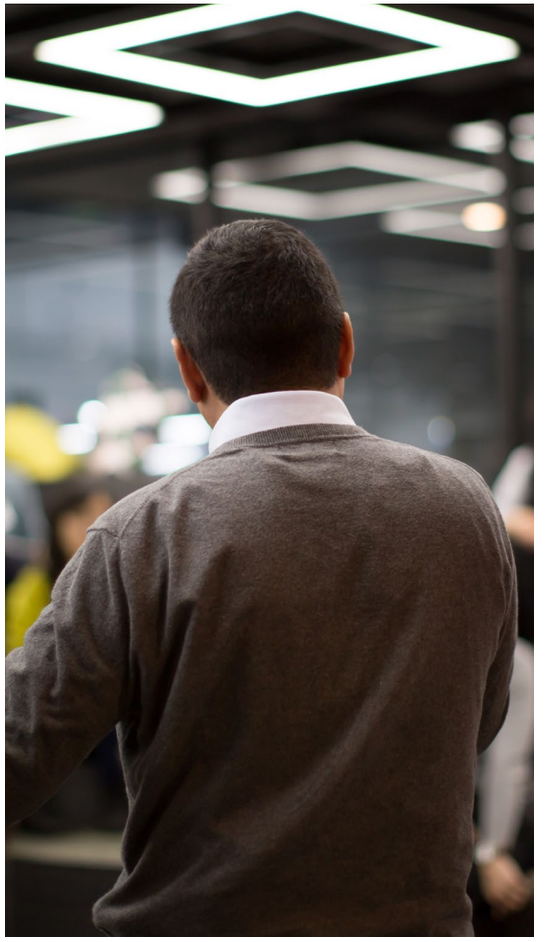
- AI security fundamentals and threat awareness module
- Responsible and ethical use of AI module
- AI policy and compliance module
- Executive and leadership AI awareness module
- AI incident recognition and reporting module
- Corporate training program development and enablement

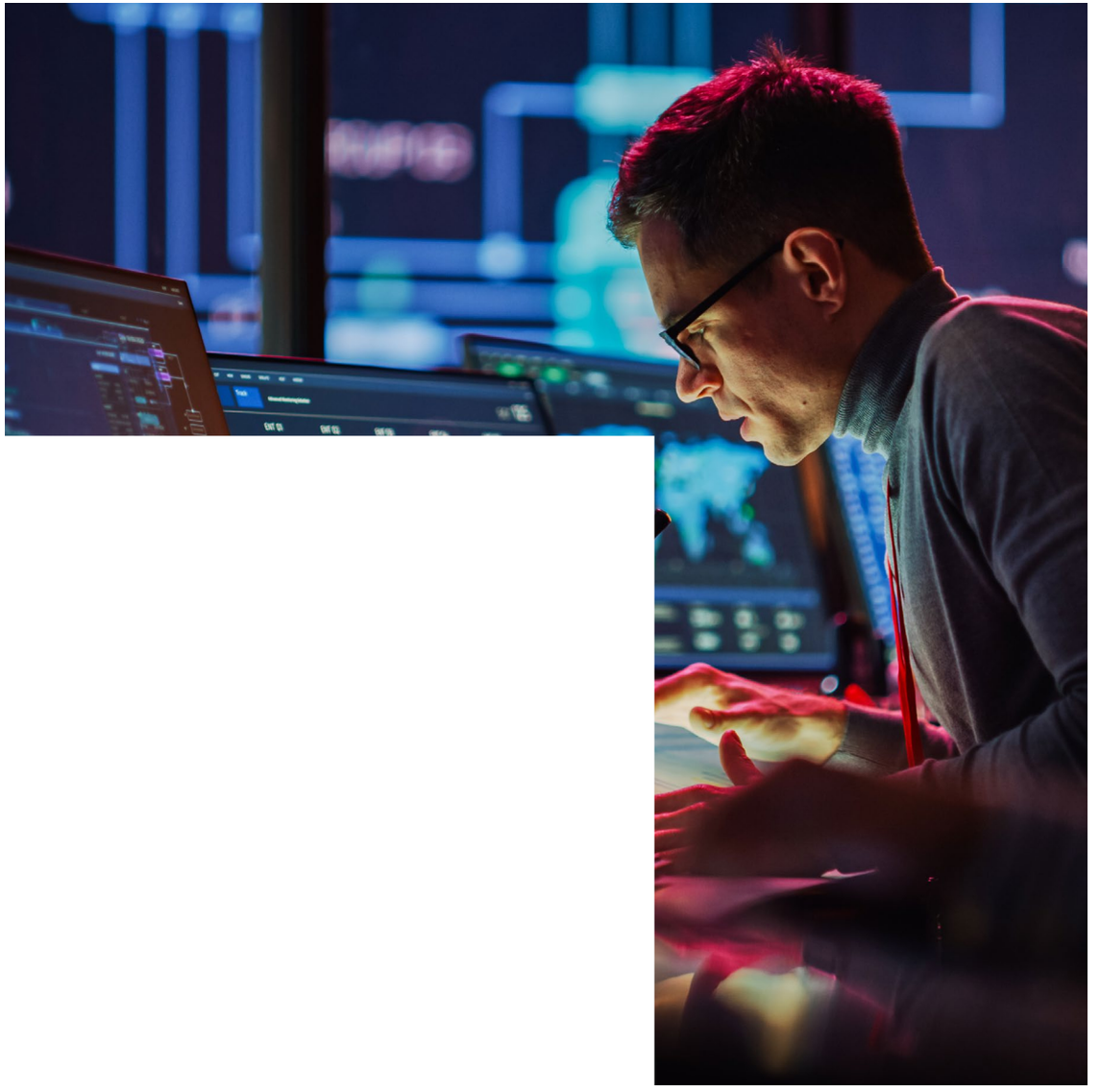
Key benefits

- Improved workforce awareness of AI-related risks
- Responsible and ethical use of AI across the organization
- Reduced likelihood of AI-related security incidents
- Executive-level understanding of AI governance responsibilities

Category

- ✓ Strategic and Technical Advisory
- ✓ Training
- ✓ Architecture and Engineering
- ✓ Managed Services and Incident Response





About our AI training

As AI becomes embedded in everyday business operations, the people using, managing and overseeing it represent both its greatest enabler and its most significant risk. Our AI security awareness training equips organizations with the knowledge to use AI securely and responsibly, delivering tailored, role-based programs that foster a strong culture of AI awareness from frontline teams to executive leadership.

Role	AI Tools	Training Module Topics
Leadership	Copilot 365, ChatGPT Enterprise, Gemini, Claude	• Use cases • Risks/ethics of use • Limitations • Pros and cons of each tool
Developers	Github Copilot, Claude Code	• Use cases • Configuration considerations • Limitations • Navigating CIA classifications • Legislative and regulatory considerations

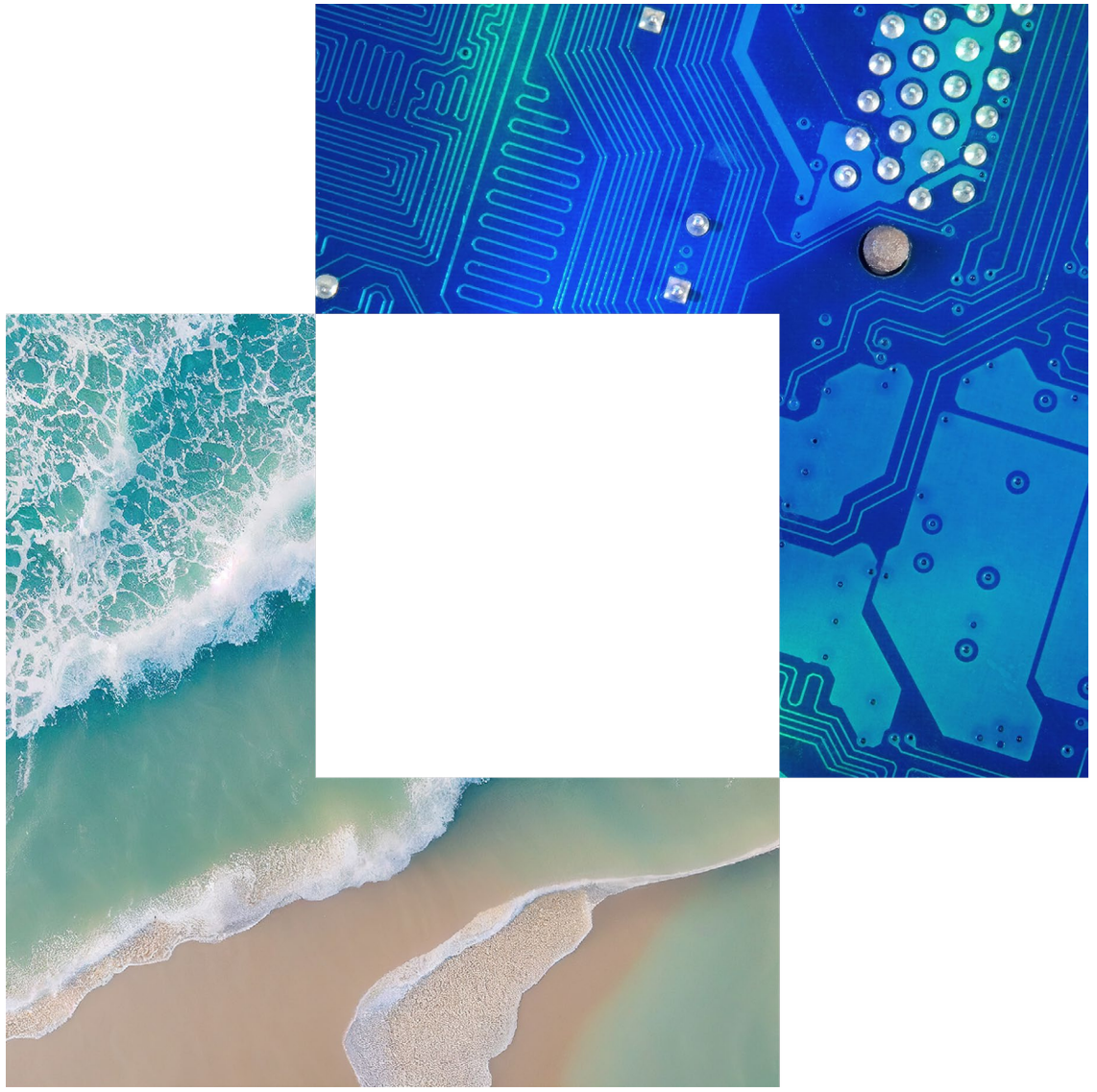
“The AI Security session delivered by CGI was a helpful and practical starting point for our team as we continue to explore the use of AI in our environment. The CGI cybersecurity consultant took the time to understand our needs and delivered the sessions with clarity and professionalism, which made the content feel relevant and accessible for our team. The sessions created space to better understand both the opportunities and the risks, while grounding the conversation in real scenarios that felt relevant to our work.

What stood out most was the balanced approach: supporting curiosity and innovation while reinforcing the importance of protecting sensitive information and using AI responsibly.

It was a valuable step in helping us build awareness and confidence as we navigate AI as an organization.”

— **Alan Brown**, Chief Operations Officer, League Data Limited

LEAGUE DATA



Why trust CGI

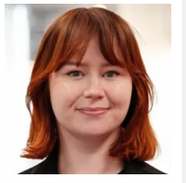
We are your partner in a world shaped by rapid technological change, including the rise of AI and its evolving security challenges. We listen, anticipate and continuously adapt to the pace at which your industry, regulatory environment and threat landscape evolve. We work alongside you to navigate complexity, secure your AI initiatives and seize new opportunities with confidence.

Responsible Use of AI Framework	As a major AI provider, we signed Canada's Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems in 2023. We have developed a framework embedded in our Management Foundation that requires all AI services and solutions we design, build or operate to adhere to three principles: Robust, Ethical and Trustworthy.
Five decades strengthening cyber resilience in Canada	Cybersecurity has been at the core of our services since CGI's founding in 1976. Our cybersecurity and AI practices are supported by hundreds of credentialed security specialists in Canada, including ISO/IEC 42001 certified auditors, serving clients across both the private and public sectors.
Strong regulatory expertise	Our business and IT experts work together to help organizations navigate evolving requirements and align with applicable laws and standards in Canada and abroad.
Proximity model	Combining local insight with global expertise, and supported by a network of 150+ technology partners worldwide, CGI tailors solutions to your AI security challenges, leveraging leading vendor innovations.
Flexible pricing	We align with each client's priorities, budget and level of maturity. Whether through fixed-price engagements, consumption-based services, or scalable managed service models, we ensure cost transparency and value at every stage.

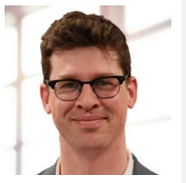
Connect with our AI governance leaders today

Let's discuss how we can help you achieve your objectives. Whether through consultation, assessment or training, CGI experts are ready to support CISOs and their teams in delivering a successful AI governance program.

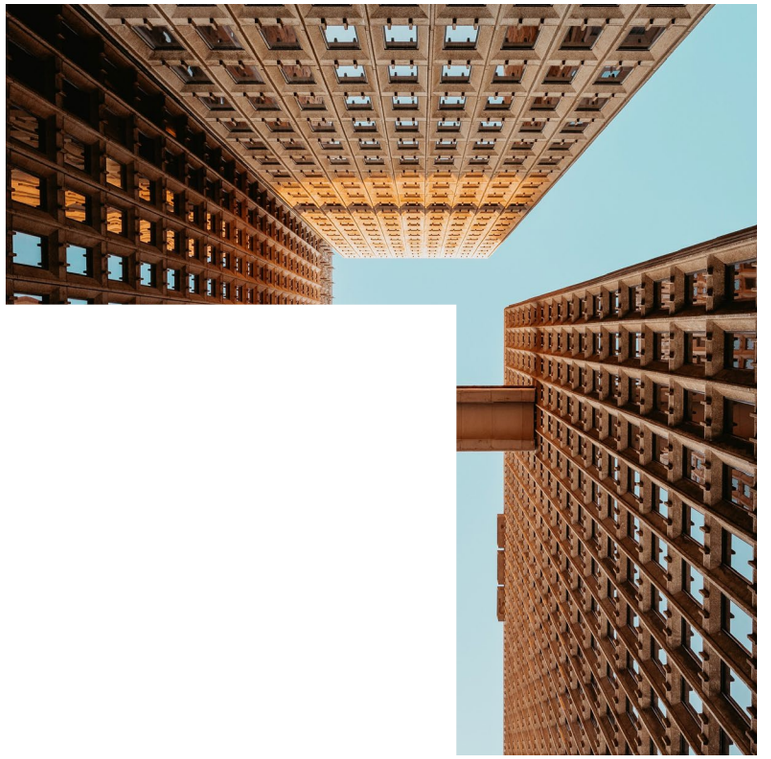
Krishna Raj Kumar
Director, Consulting Services
kr.kumar@cgi.com



Eliza Chiasson
AI Security Consultant
eliza.chiasson@cgi.com



Alex MacLaren
Senior Business Consultant
alex.maclaren@cgi.com



About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information visit: **cgi.com**