

Sécurité en IA : Services de CGI en gouvernance, risque et conformité

Faciliter l'adoption de l'IA en toute
sécurité au sein de votre organisation

Canada





Table des matières

Sommaire	3
Services de CGI en gouvernance, risque et conformité de l'IA	4
Services de conseil en réglementation et conformité de l'IA	
Développement d'un cadre de gestion des risques liés à l'IA	
Évaluation des menaces, des risques et des répercussions de l'IA sur la protection des données personnelles	
Audit interne du système de gestion de l'IA (AIMS) (ISO/IEC 42001)	
Services de conseil en sécurité et gouvernance de l'IA	
Sessions de sensibilisation à la sécurité en IA	
Pourquoi faire confiance à CGI?	15
Communiquez avec les leaders de la gouvernance de l'IA de CGI	

Sommaire

Il existe de nombreuses façons d'aborder l'intelligence artificielle (IA). Non seulement les besoins organisationnels diffèrent et changent au fil du temps, mais la technologie elle-même évolue rapidement et s'intègre de plus en plus à des plateformes de tiers.

Les innovations technologiques introduisent presque toujours de nouveaux risques en matière de sécurité, mais ceux-ci sont souvent considérés comme acceptables en raison de l'avantage concurrentiel offert. L'IA n'y échappe pas. S'il est indéniable qu'elle joue un rôle important dans la prise de décision fondée sur les données et l'efficacité opérationnelle, on constate en même temps que le fossé se creuse entre la préparation à l'IA et la sécurité des données. Plus de 75 % des organisations ont signalé des violations de sécurité liées à l'IA, mais seulement près de 30 % d'entre elles ont mis en place des pratiques efficaces de classification des données*.

La majorité des organisations ne sont pas suffisamment préparées pour réaliser leurs projets avec l'IA en toute sécurité : elles n'ont pas de stratégie cohérente en cybersécurité ni les capacités techniques nécessaires pour se défendre contre les menaces exploitant l'IA. L'émergence de l'IA agentique présente un risque encore plus important : les agents autonomes ne se contentent pas de traiter des données, ils prennent des décisions et déclenchent des actions dans plusieurs systèmes avec une supervision humaine minimale. La mauvaise utilisation des données, les biais algorithmiques, la dérive incontrôlée des modèles et les violations réglementaires ne sont plus des risques théoriques, ce sont maintenant de véritables failles présentes dans chaque déploiement de l'IA.

*[*Security Magazine, 3 Top Cybersecurity Trends from 2025, November 2025](#)*

Les organisations qui intègrent la gouvernance, la gestion des risques et la conformité dans leur stratégie en IA ne font pas que gérer les risques, elles se préparent à l'évolution continue de l'IA. En raison de l'élaboration et de la mise en œuvre de cadres réglementaires comme la loi européenne sur l'IA, la norme ISO/IEC 42001:2023 et les directives gouvernementales locales (p. ex., le projet de loi 194 en Ontario), les organisations subissent une pression croissante pour démontrer que leurs projets avec l'IA sont bien gouvernés et déployés de façon efficace, sécurisée et éthique.

CGI accompagne les organisations dans la conformité réglementaire, la modélisation des menaces, l'évaluation des risques, les audits internes et la sensibilisation du personnel aux enjeux de sécurité. Ces mesures facilitent l'adoption de l'IA à grande échelle sans faire de compromis sur la confiance, la transparence, le contrôle et le rendement des investissements.

Forte de cinq décennies d'expertise approfondie en cybersécurité, gestion des risques et services de conseil en réglementation au Canada et ailleurs, CGI transforme l'IA et ses risques en un atout stratégique et sécurisé pour les organisations.

Services de CGI en gouvernance, risque et conformité de l'IA

CGI offre six services en gouvernance, risque et conformité de l'IA pour aider les responsables de la sécurité de l'information, les responsables des données et de l'analytique ainsi que les responsables de l'IA à mettre en place les structures, les politiques et les processus nécessaires à l'encadrement responsable de l'IA de bout en bout et à faciliter l'adoption d'une IA fiable et adaptable aux exigences réglementaires de chaque secteur.



Services de conseil en réglementation et conformité de l'IA

Conseils de spécialistes pour aider la direction à mieux comprendre, schématiser et gérer proactivement les exigences de conformité liées aux initiatives en IA.

Capacités

Voici nos services :

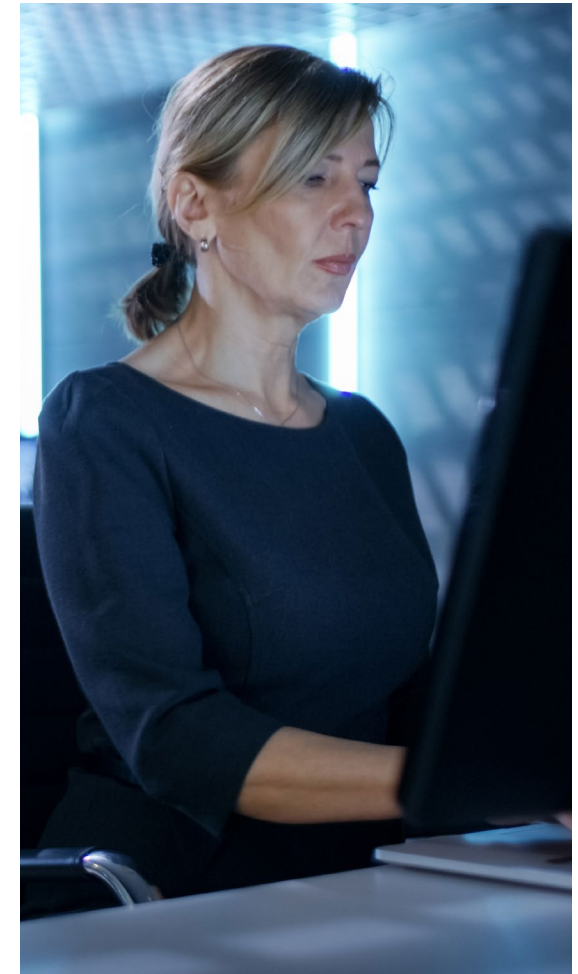
- Schématisation des exigences réglementaires et analyse des écarts
- Développement d'un cadre de conformité propre à l'IA
- Alignement sur les réglementations en matière de protection de la vie privée et des données
- Suivi de la législation en matière d'IA et veille prospective
- Analyse d'impact propre à chaque client
- Soutien à l'engagement et à la représentation

Principaux avantages

- Réduction des risques réglementaires et juridiques
- Meilleure préparation en matière de conformité
- Interprétation claire de la législation en matière d'IA
- Gouvernance de l'IA plus robuste et plus défendable

Catégorie

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident



Développement d'un cadre de gestion des risques liés à l'IA

Vue d'ensemble complète et consolidée des risques liés à l'IA grâce à des méthodologies d'évaluation rigoureuses et des outils propriétaires conçus pour les environnements d'IA.

Capacités

Voici nos services :

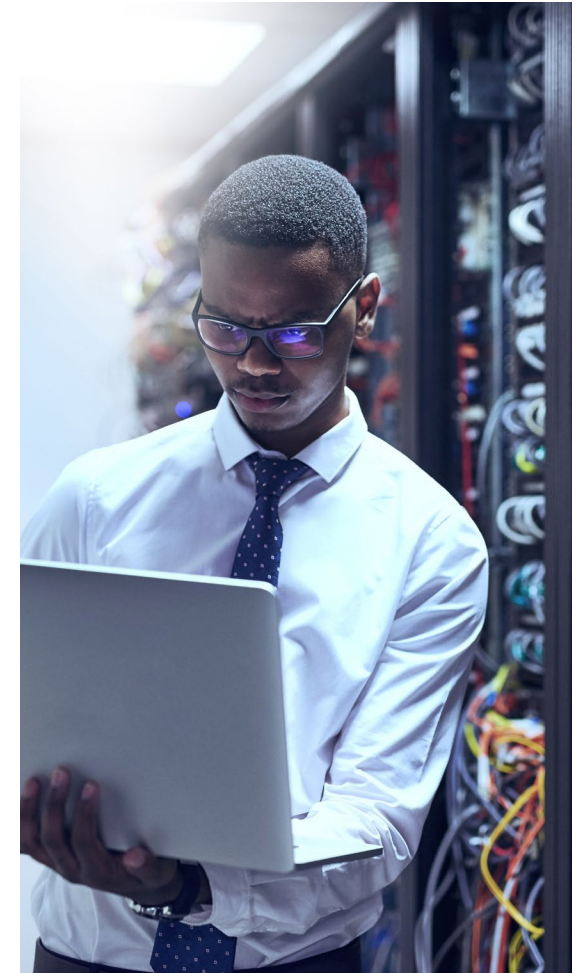
- Adoption et personnalisation de cadres actuels
- Développement de cadres sur mesure
- Intégration de cadres
- Révisions et mises à jour continues
- Modélisation sur mesure des menaces liées à l'IA

Principaux avantages

- Identification et atténuation globales des risques liés à l'IA
- Intégration aux cadres de cybersécurité de l'entreprise
- Amélioration continue des processus de gestion des risques liés à l'IA
- Résilience renforcée face aux nouvelles menaces liées à l'IA

Catégorie

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident



Évaluation des menaces, des risques et des répercussions de l'IA sur la protection des données personnelles

L'élaboration d'une approche structurée pour identifier, atténuer et gérer les risques liés à l'IA en combinant des cadres de référence de pointe avec des méthodologies de modélisation des menaces sur mesure et adaptées à votre environnement.

Capacités

Voici nos services :

- Évaluation des menaces et des risques liés à l'IA
- Évaluation des répercussions de l'IA sur la protection des données personnelles
- Outils propriétaires d'évaluation de l'IA

Principaux avantages

- Notation claire des risques et conseils de correction
- Identification des vulnérabilités dans l'architecture de l'IA
- Amélioration de la protection et de la conformité en matière de données personnelles
- Informations exploitables pour les équipes de sécurité

Catégorie

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident



Audit interne du système de gestion de l'IA (AIMS) (ISO/IEC 42001)

Audit interne de vos systèmes d'IA mené par des spécialistes, y compris une évaluation rigoureuse des politiques, processus, contrôles et structures de gouvernance nécessaires pour vous conformer à la norme ISO/IEC 42001:2023.

Capacités

Voici nos services :

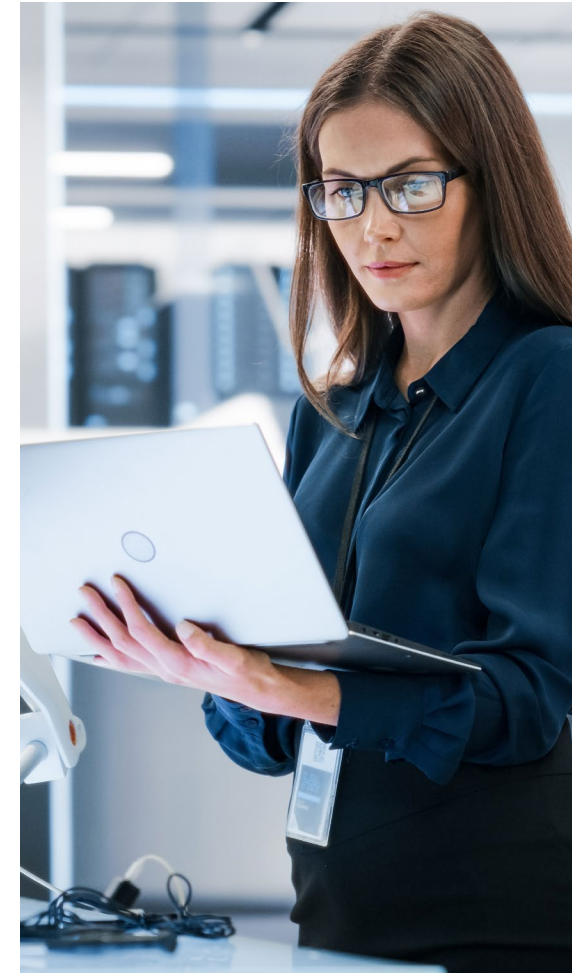
- Évaluation de la préparation à la certification ISO/IEC 42001
- Audit interne du système de gestion de l'IA (AIMS)
- Revue des politiques et des contrôles
- Évaluation des objectifs et de la performance en matière d'IA
- Soutien aux mesures correctives et à l'amélioration continue

Principaux avantages

- Meilleure préparation à la certification ISO/IEC 42001
- Feuille de route claire pour corriger les cas de non-conformité
- Gouvernance et imputabilité renforcées
- Engagement démontré envers l'utilisation responsable de l'IA

Catégorie

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident



Qu'est-ce que la certification ISO/IEC 42001:2023?

Selon l'Organisation internationale de normalisation (ISO), « ISO/IEC 42001 est une norme internationale qui spécifie les exigences pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de l'intelligence artificielle (SMIA) au sein d'un organisme. Elle est conçue pour permettre aux organismes proposant ou utilisant des produits ou des services sollicitant une IA de veiller au développement et à l'utilisation des systèmes d'IA de manière responsable. »

L'ISO définit également le SMIA comme un « ensemble d'éléments corrélés ou en interaction au sein d'un organisme, utilisés pour établir des politiques et des objectifs, ainsi que des processus à l'appui de l'atteinte des objectifs fixés, afin de développer, fournir ou utiliser des systèmes d'IA de manière responsable. »

L'ISO a élaboré plusieurs normes pour aider les organisations à atténuer les risques et à maximiser les avantages de l'IA, notamment la norme ISO/IEC 23894. La principale différence entre celle-ci et ISO/IEC 42001 réside dans leur champ d'application. La norme ISO/IEC 23894 adapte les normes générales de gestion des risques (ISO 38001-2018) à l'IA, tandis que la norme ISO/IEC 42001 se concentre sur la manière dont les organisations conçoivent, adoptent et documentent leurs procédures opérationnelles internes pour gérer les systèmes d'IA.

Quels sont les principaux avantages de la mise en œuvre de la norme ISO/IEC 42001?

- Reconnaissance internationale : la norme ISO/IEC 42001 est reconnue à l'échelle internationale; elle est particulièrement utile pour les organisations multinationales.
- IA responsable : favoriser une utilisation éthique et responsable de l'IA.
- Gestion de la réputation : renforcer la confiance dans les applications d'IA.
- Gouvernance de l'IA : assurer la conformité aux exigences juridiques et réglementaires.

- Conseils pratiques : fournir une approche structurée pour gérer efficacement les risques propres à l'IA.
- Identification des possibilités : encourager l'innovation dans un cadre structuré.

Source: [ISO/IEC 42001:2023 – AI management systems](#)

Quelles sont les recommandations présentées aux organisations dans l'annexe A?

L'annexe A décrit 38 contrôles répartis dans neuf domaines.

Domaine	Nom	Description du contrôle
A.2	Politiques relatives à l'IA	Exigences relatives à la documentation d'une politique sur l'IA et à son alignement sur les autres politiques de l'entreprise (p. ex., confidentialité, sécurité).
A.3	Organisation interne	Définition des rôles et responsabilités (p. ex., responsable de l'éthique de l'IA) et mise en place de processus pour signaler les préoccupations liées à l'IA.
A.4	Ressources pour les systèmes d'IA	Documentation des ressources techniques, humaines, informatiques et relatives aux données qui sont utilisées dans l'ensemble du cycle de vie des systèmes d'IA.
A.5	Évaluation des répercussions des systèmes d'IA	Processus obligatoires pour évaluer les répercussions de l'IA sur les individus, la société et les droits de la personne (analyse d'impact).
A.6	Cycle de vie des systèmes d'IA	Contrôles couvrant l'ensemble du cycle de vie des systèmes d'IA : conception, développement, vérification, validation, déploiement et mise hors service.
A.7	Données pour les systèmes d'IA	Normes concernant la qualité, l'acquisition, la traçabilité (provenance), la préparation et le nettoyage des données.
A.8	Informations pour les parties prenantes	Exigences en matière de transparence, notamment l'obligation d'informer les utilisateurs/utilisatrices et les organismes de réglementation sur le fonctionnement et les limites des systèmes d'IA.
A.9	Utilisation des systèmes d'IA	Règles pour utiliser l'IA de façon responsable, notamment en assurant une supervision humaine et en évitant une dérive des objectifs.
A.10	Relations avec les tiers et les clients	Contrôles pour gérer les risques liés aux modèles externes (p. ex., ChatGPT, Gemini) et aux fournisseurs tiers de services d'IA.
Communiquez avec notre équipe pour discuter des manières dont nous pouvons vous aider à mettre en œuvre ces recommandations.		

Services de conseil en sécurité et gouvernance de l'IA

Établir des bases solides de gouvernance et des pratiques d'utilisation responsable de l'IA à l'échelle de votre organisation.

Capacités

Voici nos services :

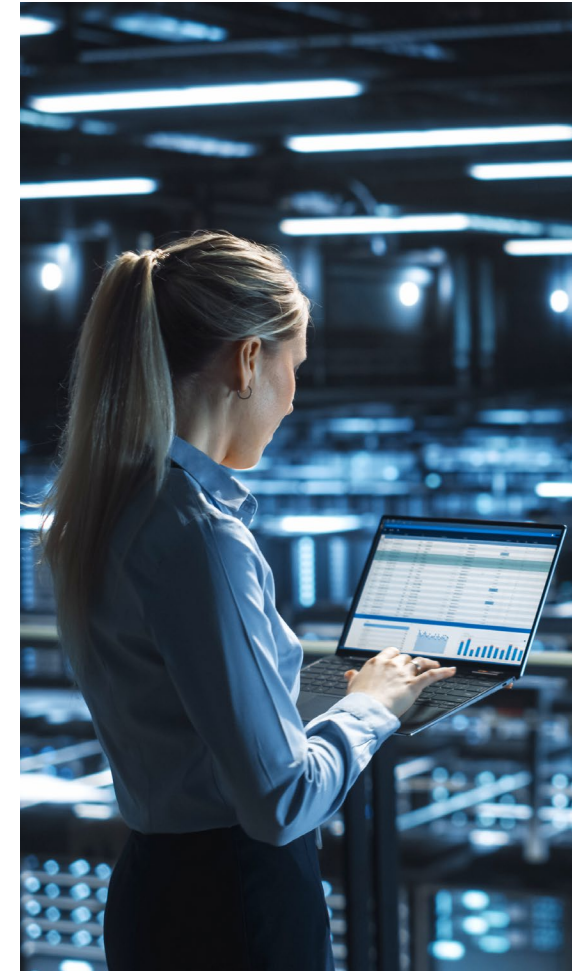
- Évaluation de la maturité en matière de gouvernance de l'IA
- Conception d'un cadre de gouvernance
- Élaboration de politiques sur l'IA
- Préparation à l'adoption de l'IA et conseils sur son utilisation responsable

Principaux avantages

- Structure de gouvernance claire et imputabilité
- Déploiement responsable et éthique de l'IA
- Alignement entre les initiatives en IA et les objectifs d'affaires
- Renforcement de la confiance quant à l'adoption de l'IA

Catégorie

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident



Sessions de sensibilisation à la sécurité en IA

Programmes de formation adaptés aux rôles et conçus pour favoriser l'utilisation de l'IA de manière sécurisée, responsable et éthique à tous les niveaux de l'organisation, des équipes de première ligne aux équipes de direction.

Capacités

Voici nos services :

- Module sur les principes fondamentaux de la sécurité en matière d'IA et la sensibilisation aux menaces
- Module sur l'utilisation responsable et éthique de l'IA
- Module sur les politiques et la conformité en matière d'IA
- Module de sensibilisation à l'IA destiné aux équipes de direction
- Module sur la reconnaissance et le signalement des incidents liés à l'IA
- Élaboration et mise en place de programmes de formation en entreprise

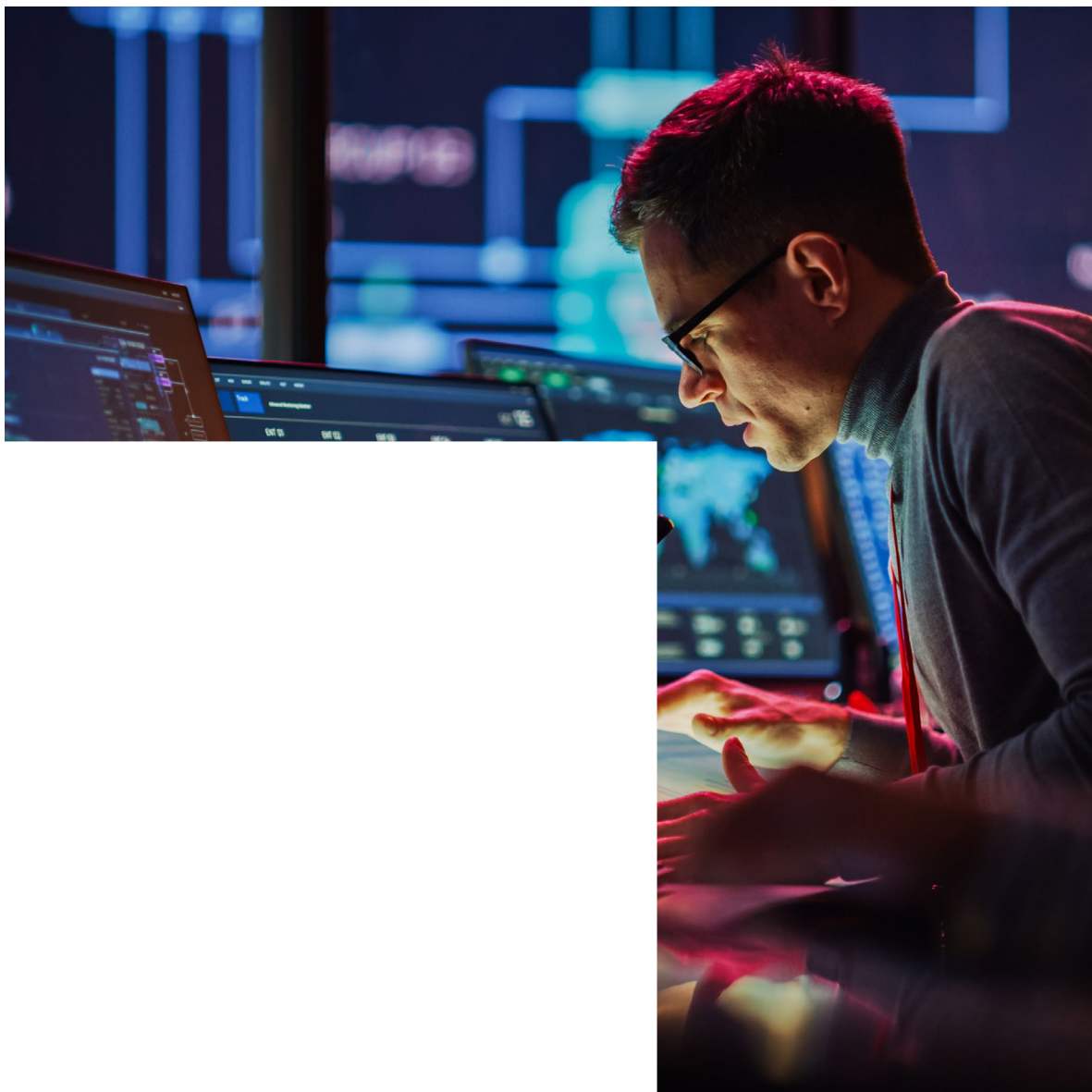
Principaux avantages

- Sensibilisation accrue du personnel face aux risques liés à l'IA
- Utilisation responsable et éthique de l'IA à l'échelle de l'organisation
- Réduction de la probabilité d'incidents de sécurité liés à l'IA
- Compréhension des équipes de direction quant aux responsabilités en matière de gouvernance de l'IA

Category

- ✓ Conseils stratégiques et techniques
- ✓ Formation
- ✓ Architecture et ingénierie
- ✓ Services en mode délégué et intervention en cas d'incident





Au sujet de notre formation en IA

Dans un contexte d'intégration croissante de l'IA dans les activités courantes des entreprises, les personnes qui utilisent cette technologie, la gèrent ou la supervisent constituent à la fois son principal accélérateur et son principal risque. Nos sessions de sensibilisation à la sécurité en IA fournit aux organisations les connaissances nécessaires pour utiliser l'IA de manière sécurisée et responsable. Nos programmes sont adaptés aux rôles et renforcent une culture de sensibilisation à l'IA à tous les niveaux de l'organisation, des équipes de première ligne aux équipes de direction.

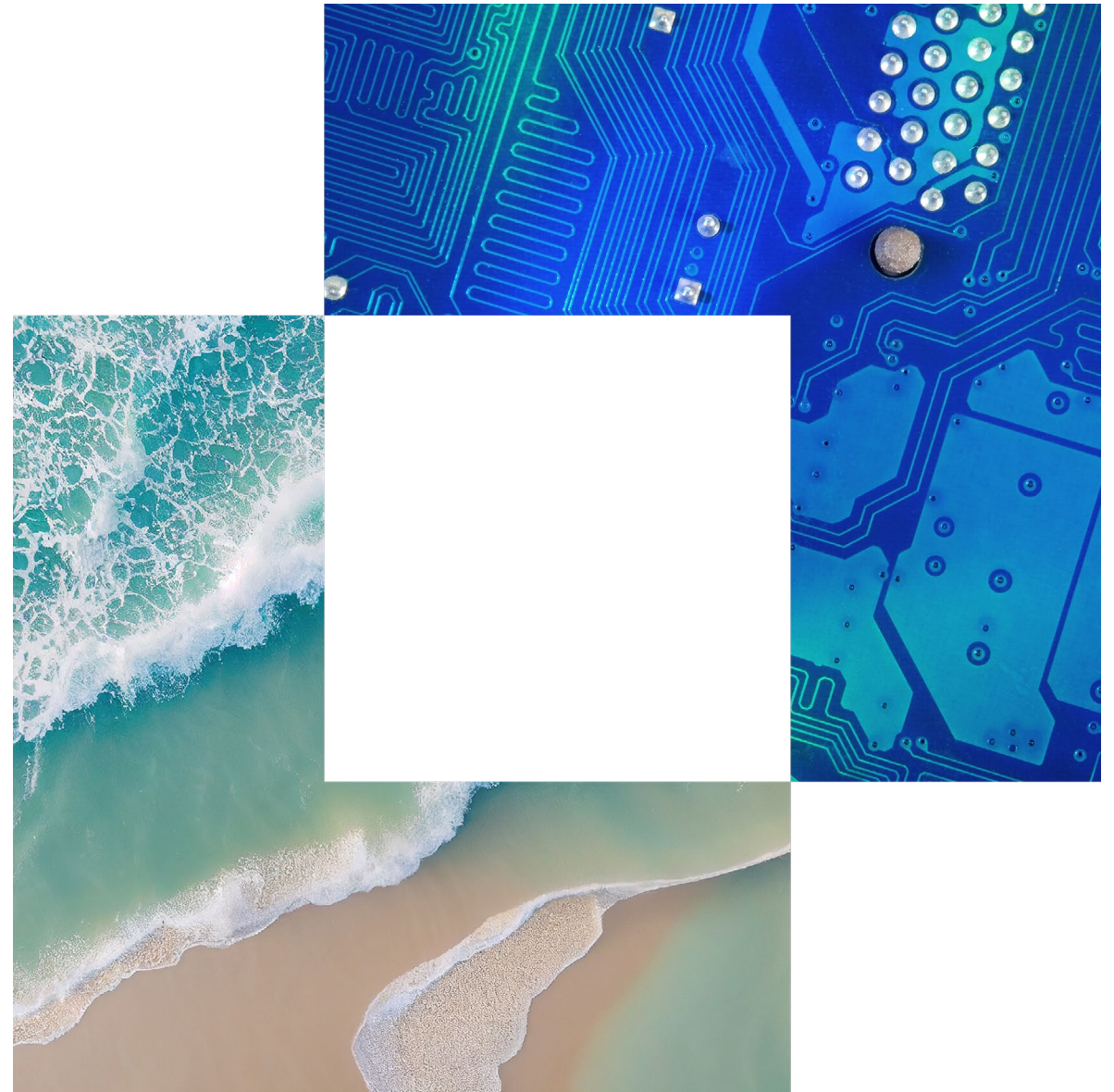
Rôle	Outils d'IA	Sujets des modules de formation
Équipe de direction	Copilot 365, ChatGPT Enterprise, Gemini, Claude	• Cas d'utilisation • Risques et enjeux éthiques • Limites • Points positifs et négatifs de chaque outil
Équipe de développement	Github Copilot, Claude Code	• Cas d'utilisation • Enjeux de configuration • Limites • Comprendre les classifications de sécurité basées sur la confidentialité, l'intégrité et la disponibilité des données • Enjeux législatifs et réglementaires

« Les séances de CGI sur la sécurité de l'IA présentaient un bon point de départ pour l'exploration pratique des cas d'utilisation de l'IA dans notre environnement. La personne-ressource de CGI en cybersécurité a pris le temps de bien cerner nos besoins et a animé les séances avec clarté et professionnalisme. Le contenu était pertinent et accessible pour notre équipe. Les séances nous ont permis de mieux comprendre à la fois les possibilités et les risques grâce à l'introduction de scénarios réels et pertinents pour notre travail.

Ce qui a le plus retenu notre attention, c'est l'approche équilibrée adoptée qui a encouragé la curiosité et l'innovation tout en soulignant Cette formation importante a renforcé notre sensibilisation et notre confiance dans notre exploration de l'IA en tant qu'organisation.

Cette formation importante a renforcé notre sensibilisation et notre confiance dans notre exploration de l'IA en tant qu'organisation. »

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



Pourquoi faire confiance à CGI?

CGI est votre partenaire de choix dans un contexte marqué par des changements technologiques rapides, notamment l'essor de l'IA et les défis de sécurité qui en découlent. L'objectif de CGI est d'être à votre écoute, d'anticiper l'évolution de votre secteur d'activité, du cadre réglementaire et des menaces, puis de s'y adapter. CGI vous aide à composer avec cette complexité, à sécuriser vos projets d'IA et à saisir de nouvelles occasions en toute confiance.

Cadre d'utilisation responsable de l'IA	En tant que grand fournisseur de services utilisant l'IA, CGI a signé en 2023 le Code canadien de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés. CGI a élaboré un cadre de travail, qui est intégré dans ses Assises de gestion, requérant que les services et solutions d'IA qu'elle conçoit, crée ou exploite respectent les trois principes suivants : robustesse, éthique et fiabilité.
Cinq décennies à renforcer la cyberrésilience au Canada	La cybersécurité est au cœur des services de CGI depuis sa fondation en 1976. Ses pratiques en cybersécurité et en IA sont soutenues par des centaines de spécialistes certifié(e)s en sécurité au Canada, y compris des auditeurs et auditrices avec la certification ISO/IEC 42001, au service de clients des secteurs public et privé.
Solide expertise en réglementation	Ses spécialistes dans le domaine des affaires et des TI collaborent pour aider les organisations à se conformer aux exigences, aux lois applicables et aux normes changeantes au Canada et ailleurs.
Modèle de proximité	En tirant parti de sa connaissance des marchés locaux, de son expertise mondiale, de son réseau de plus de 150 partenaires technologiques dans le monde et des innovations des principaux fournisseurs, CGI élabore des solutions sur mesure pour relever vos défis de sécurité en IA.
Tarification flexible	CGI s'adapte aux priorités, au budget et au niveau de maturité de chaque client. Qu'il s'agisse d'une entente à prix fixe, de services facturés à l'utilisation ou de modèles de services évolutifs en mode délégué, CGI garantit la transparence des coûts et une valeur ajoutée à chaque étape.

Communiquez avec les leaders de la gouvernance de l'IA de CGI

Découvrez comment CGI peut vous aider à atteindre vos objectifs. CGI est prête à accompagner les responsables de la sécurité de l'information et leurs équipes dans la mise en œuvre de programmes de sécurité robustes en IA dans le cadre de services de conseil stratégique, d'évaluations ou de formations.



Krishna Raj Kumar
Directeur, services-conseils
kr.kumar@cgi.com



Eliza Chiasson
Conseillère, sécurité en IA
eliza.chiasson@cgi.com



Alex MacLaren
Conseiller principal en management
alex.maclaren@cgi.com

À propos de CGI

Allier savoir et faire

Fondée en 1976, CGI figure parmi les plus importantes entreprises de services de conseil en technologie de l'information (TI) et en management au monde.

Nous sommes guidé(e)s par les faits et axé(e)s sur les résultats afin d'accélérer le rendement de vos investissements. Pour nos 21 secteurs d'activité et à partir de plus de 400 sites à l'échelle mondiale, nos 94 000 professionnels et professionnelles offrent des services de conseil complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en œuvre à l'échelle locale.

Pour en savoir plus

Visitez [cgi.com](https://www.cgi.com)

