Obligations des compagnies privées / organisations publiques

Lois/ Règlements/ Standards applicables (ISO – Information Security)	**Activités/ livrables à réaliser (obligations)**	**Risques relies au statut quo (non réalisation et/ ou non-respect)**	**Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)**
Loi 25 et projet de loi 64 (Loi sur la protection des renseignements personnels dans le secteur privé (Loi sur le privé) : **Nouvelles dispositions protégeant la vie privée des Québécois - Certaines dispositions entrant en vigueur le 22 septembre 2022** (Rappelons que les modifications apportées par la Loi 25 sont entrées progressivement en vigueur sur une période de trois ans, jusqu'en 2024. La prochaine date à retenir est le 22 septembre 2023)	*En plus de respecter les obligations actuelles en matière de protection des renseignements personnels, les **entreprises** doivent notamment:* • En cas d'incident de confidentialité, tenir un registre de tous les incidents **et prendre rapidement des mesures** afin de diminuer le risque qu'un préjudice soit causé aux personnes concernées. Une entreprise doit aussi aviser la Commission et les personnes concernées de tout incident présentant un risque sérieux de préjudice; • En plus de ces obligations, les **organismes publics** devront aussi former un comité sur l'accès à l'information et la protection des renseignements personnels.	Absence de prises de mesures raisonnables pour diminuer les risques qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent Ne pas aviser la Commission d'accès à l'information et la personne concernée si l'incident présente un risque de préjudice sérieux; Ne pas tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande;	Depuis le 22 septembre 2022 La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation des 3 activités suivantes • *Faites l'inventaire des renseignements personnels détenus par votre entreprise (ou pour son compte par un tiers) et évaluez leur sensibilité;* • *Mettez en place des mesures pour prévenir ou limiter les conséquences d'un incident de confidentialité impliquant un renseignement personnel;* • *Instaurez des pratiques qui vous permettront de réagir adéquatement et rapidement en cas d'incident de confidentialité impliquant un renseignement personnel (ex. : plan de réponse aux incidents et directive au personnel);* Depuis le 22 septembre 2023 La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
			réalisation de l'activité suivante • *Établir et mettre en œuvre vos politiques de gouvernance en matière de protection des renseignements personnels qui nécessitera l'inventaire réalisé ci-dessus et la précision des rôles et responsabilités des membres du personnel* <u>Depuis le 22 septembre 2024</u> Les 9 outils de gestion de projet de PIGA-TI ainsi que les standards ISO applicables permettront de définir, justifier, planifier, gérer et suivre la réalisation des bénéfices des projets reliés à l'arrivée des nouveaux systèmes et des versions futures Et la gestion de changement TI et le plan de relève (pour les sites de production et de relève exploités) de PIGA-TI ainsi que les standards ISO applicables aideront à la réalisation de l'activité suivante 1. *Informez l'équipe responsable de l'entretien, de la mise à jour ou du développement de vos systèmes informatiques que vous avez de nouveaux besoins*

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
			d'affaires en lien avec le droit à la portabilité des renseignements personnels, à savoir : *o que vos systèmes permettent de communiquer, sur demande d'une personne concernée, un renseignement personnel informatisé recueilli auprès d'elle, et ce, dans un format technologique structuré et couramment utilisé;* *o que cette communication puisse également se faire à une personne ou à un organisme autorisé par la Loi à recueillir le renseignement, à la demande de la personne concernée.*
Loi 38 et projet de Loi 38 **(LOI MODIFIANT LA LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT ET D'AUTRES DISPOSITIONS LÉGISLATIVES)** adopté le 5 décembre 2023 (mesures concrètes	« Avec l'adoption du projet de loi nº 38, l'administration publique se dote d'outils importants pour assurer une gouvernance cohérente de la transformation numérique de l'État. En effet, par les dispositions prises dans la loi, nous nous assurons d'identifier clairement les priorités gouvernementales en la matière afin d'offrir une vision commune, claire, cohérente et engagée dans le virage numérique de l'État, tant pour les organismes publics que les citoyens. »		

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
pour assurer la cybersécurité et la transformation numérique de l'administration publique Québécoise)	**Principales modifications** *Article 5.1* Un organisme public doit appliquer les orientations, les stratégies, les politiques, les standards, les directives, les règles ou les indications d'application pris en vertu de la présente loi. La responsabilité du respect de cette obligation incombe au dirigeant de l'organisme public, qui doit prendre des moyens pour la faire connaître et respecter par les membres du personnel de celui-ci. *Article 12.5.1* Le ministre peut, par arrêté, prévoir l'obligation pour un organisme public qu'il désigne de recourir à ses services pour réaliser des activités de cybersécurité, selon les conditions et modalités qu'il détermine. *Article 12.5.2* Le ministre peut, par tout moyen et dans l'objectif de soutenir un organisme public en cas d'atteinte ou de risque d'atteinte visé au deuxième alinéa de l'article 12.2, lui ordonner de retirer de ses infrastructures ou de ses systèmes tout logiciel, toute application ou tout autre actif informationnel qu'il détermine *Article 12.8.1* Le ministre propose annuellement au gouvernement, dans les 60 jours suivant le dépôt	Si non-respect, investissements informationnels supplémentaires requis afin d'assurer le remplacement des systèmes associés ou leur intégration à la pièce sans vision globale	La gouvernance globale de PIGA-TI et les standards ISO applicables permettront d'associer les orientations, les stratégies, les politiques, les standards, les directives, les règles à toutes ou à certaines activités d'affaires afin d'assurer leur respect lors de l'exécution de celles-ci et des projets leur étant associés La discipline d'architecture de PIGA-TI et les standards ISO applicables assureront d'intégrer (ou retirer) avec rigueur les nouveaux standards informationnels découlant des décisions d'investissements du gouvernement. Les impacts potentiels de ces décisions pourront être évaluées plus facilement au préalable si demandés par le gouvernement La gouvernance de gestion de portefeuille de PIGA-TI et les standards ISO applicables aideront à définir, justifier et faire approuver les investissements informationnels détaillés à l'aide de la discipline d'architecture de PIGA-TI Les 9 outils de gestion de projet de PIGA-TI ainsi que

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	à l'Assemblée nationale du plan des investissements et des dépenses en matière de ressources informationnelles des organismes publics visé à l'article 16.1, un portefeuille des projets prioritaires en ressources informationnelles afin que soient établies les priorités gouvernementales au regard des initiatives de transformation numérique des organismes publics *Article 12.8.2* Le ministre présente au gouvernement, au moment qu'il juge opportun, la consolidation des états d'avancement des projets en ressources informationnelles des organismes publics visés par le portefeuille des projets prioritaires **Impacts sur d'autres lois** LOI SUR LE MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE *Article 2* Le ministre doit assurer la cohérence et l'harmonisation des actions gouvernementales dans les domaines de la cybersécurité et du numérique et, à cette fin, être associé à l'élaboration des mesures ainsi qu'aux décisions ministérielles dans ces domaines et donner son avis lorsqu'il le juge opportun	Si non-respect, investissements informationnels supplémentaires requis afin d'assurer le remplacement des systèmes associés ou leur intégration à la pièce sans vision globale	les standards ISO applicables permettront, en complémentarité avec la gouvernance de gestion de portefeuille, de définir, justifier, planifier, gérer et suivre la réalisation des bénéfices des projets reliés à l'arrivée des nouveaux systèmes et des versions futures Et la gestion de changement TI et le plan de relève (pour les sites de production et de relève exploités) de PIGA-TI ainsi que les standards ISO applicables aideront à l'entretien et à la mise à jour des systèmes informatiques associés aux investissements informationnels approuvés par la gouvernement Les mêmes outils de PIGA-TI et ISO décrits ci-dessus sont applicables

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	Article 4 Le ministre peut fournir à un organisme public tout autre service en ressources informationnelles en vue de répondre à un besoin particulier d'un tel organisme lorsque ce dernier lui en formule la demande *Article 5.1* Le ministre fournit aux organismes publics les services de certification, incluant les services de répertoire y afférents, ainsi que les services de signature électronique que le gouvernement détermine. Un décret pris en vertu du premier alinéa détermine les services visés, les conditions et modalités de leur fourniture ainsi que les cas et les conditions selon lesquels un organisme public est tenu d'y recourir pour répondre à ses besoins. Il peut autoriser le ministre à déléguer certaines fonctions relatives aux services à un organisme public. Pour permettre sa mise en œuvre, il peut également prévoir le transfert au ministre d'actifs informationnels d'un organisme public ainsi que de toutes les obligations qui en résultent *Article 10.1* Le gouvernement peut autoriser la mise en œuvre par le ministre d'un projet pilote visant à étudier, à expérimenter ou à innover dans		

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	le domaine de la cybersécurité ou dans celui du numérique, ou à définir des normes applicables en de tels domaines. Un tel projet pilote peut viser les organismes publics ou les entreprises du gouvernement au sens de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), toute autre entreprise ou les citoyens. Dans le respect des dispositions législatives applicables, notamment en matière de protection des renseignements personnels et de la vie privée, le gouvernement détermine les normes et les obligations applicables dans le cadre d'un projet pilote. Il détermine également les mécanismes de surveillance et de reddition de comptes applicables dans le cadre d'un projet pilote. Un projet pilote est établi pour une durée maximale de trois ans, que le gouvernement peut prolonger d'au plus un an. Le gouvernement peut, en tout temps, modifier un projet pilote ou y mettre fin. Les résultats du projet pilote doivent être publiés sur le site Internet du ministère de la Cybersécurité et du Numérique au plus tard un an après la fin du projet pilote.		

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	LOI SUR LE MINISTÈRE DE LA JUSTICE *Article 32.1* L'article 32.1 de la Loi sur le ministère de la Justice (chapitre M-19) est modifié par la suppression, dans le paragraphe 2°, de « à la certification requise pour assurer la sécurité des échanges électroniques impliquant le gouvernement, ses ministères et ses organismes, dans le cadre de fonctions qui ont été déléguées en application de l'article 66 de la Loi sur l'administration publique (chapitre A-6.01), ou	Si non-respect, investissements informationnels supplémentaires requis afin d'assurer le remplacement des systèmes associés ou leur intégration à la pièce sans vision globale	Les mêmes outils de PIGA-TI et ISO décrits ci-dessus sont applicables
Loi 27 et projet de loi C-27 (déposé à la chambre des communes le 4 novembre 2022) : Loi fédérale édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois	Section 2.2.4 – Responsabilités des organisations Suivant la LPVPC, toute organisation est responsable des renseignements personnels qui relèvent d'elle. Les renseignements relèvent d'une organisation lorsque celle-ci établit les fins pour lesquelles ils sont recueillis, utilisés ou communiqués. La LPVPC précise que l'organisation conserve cette responsabilité même si un fournisseur de services mène les activités pour elle. Les obligations prévues à la LPVPC ne s'appliquent pas au fournisseur de services pour ce qui est des renseignements qui lui sont transférés par une organisation (sauf s'il les recueille, utilise ou communique à d'autres fins que celles pour lesquelles ils lui ont	Incompréhension des renseignements personnels en inventaire et de leur utilisation pouvant causer des préjudices graves à des individus ou des organisations	La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation de l'activité ci-contre

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	été transférés). L'organisation s'assure également que tout fournisseur de services à qui elle transfère des renseignements personnels offre une protection équivalente à celle qu'elle offre elle-même (art. 7 et 11). Chaque organisation désigne au moins un individu chargé des questions relatives aux obligations de l'organisation sous le régime de la LPVPC et elle met en œuvre et tient à jour un programme de gestion de la protection des renseignements personnels (le programme). Ce programme comprend les politiques, pratiques et procédures que l'organisation a mises en place pour se conformer aux obligations qui lui incombent en vertu de la LPVPC. Il tient compte du volume et de la nature sensible des renseignements personnels qui relèvent de l'organisation (art. 8 et 9). Par exemple, les renseignements personnels des mineurs sont toujours considérés comme étant de nature sensible (par. 2(2)). L'organisation donne aussi accès au contenu du programme au commissaire, lorsque ce dernier en fait la demande. Le commissaire peut fournir des conseils ou recommander des mesures correctives à l'organisation après avoir examiné le programme (art. 10). **2.2 Loi sur la protection de la vie privée des consommateurs et**	En l'absence d'un responsable, non-respect des obligations identifiées pouvant causer des préjudices graves à des individus ou des organisations	La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation de l'activité ci-contre

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	autres dispositions (art. 2 du projet de loi) Section 2.2.9 – Mesures de sécurité Sous le régime de la LPVPC, une organisation doit protéger les renseignements personnels qu'elle détient. La protection se fait au moyen de mesures de sécurité matérielles, organisationnelles ou techniques, et le degré de protection doit être proportionnel à la nature sensible de ces renseignements. Les mesures doivent également tenir compte de la quantité de renseignements et de leur répartition, format et méthode de stockage (art. 57). La LPVPC reprend également le contenu des articles 10.1 à 10.3 de la LPRPDE, qui prévoient un régime de déclaration d'atteinte aux mesures de sécurité (art. 58 à 60). Ce régime fait en sorte qu'une organisation doit déclarer au commissaire toute atteinte aux mesures de sécurité concernant des renseignements personnels qui relèvent d'elle, lorsqu'il est	Protection inadéquate des renseignements personnels en inventaire et de leur utilisation pouvant causer des préjudices graves à des individus ou des organisations Non divulgation des incidents de sécurité et	Les 10 outils de gestion de projet de PIGA-TI ainsi que les standards ISO applicables permettront de justifier, planifier, gérer et suivre la réalisation des bénéfices des projets reliés à l'arrivée des nouveaux systèmes et des versions futures Et la gestion de changement TI et le plan de relève (pour les sites de production et de relève exploités) de PIGA-TI ainsi que les standards ISO applicables aideront à la réalisation de l'activité ci-contre Et Le plan de relève de PIGA-TI et les standards ISO applicables aideront à la réalisation des activités identifiées ci-contre pour les sites de production et de relève exploités La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	« raisonnable de croire que, dans les circonstances, l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu ». Elle avise également l'individu concerné dès que possible (art. 58). Un préjudice grave peut prendre différentes formes, comme la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations et la perte financière (par. 58(7)). L'organisation qui avise un individu d'une atteinte aux mesures de sécurité le concernant en avise aussi toute autre organisation ou institution gouvernementale qui peut être en mesure de réduire le risque de préjudice pouvant résulter de cette atteinte ou d'atténuer ce préjudice (art. 59). Elle tient un registre des atteintes aux mesures de sécurité qui ont trait à des renseignements personnels et en donne l'accès au commissaire, à la demande de ce dernier (art. 60). Tout fournisseur de services qui conclut à une atteinte aux mesures de sécurité ayant trait à des renseignements personnels en avise dès que possible l'organisation de laquelle ces renseignements relèvent (art. 61). **2.5 Loi sur l'intelligence artificielle et les données (art. 39 du projet de loi)** Section 2.5.1 Champ d'application	préjudices graves à l'endroit d'individus ou d'organisations Absence d'un registre identifiant les mesures d'atténuation aux risques de préjudice identifiés	réalisation de l'activité ci-contre La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation de l'activité ci-contre

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	Le champ d'application de la Loi sur l'IA se limite au secteur privé, dans le cadre des échanges ou du commerce internationaux ou interprovinciaux liés aux systèmes d'IA. Ainsi, elle ne s'applique pas aux institutions fédérales au sens de l'article 3 de la *Loi sur la protection des renseignements personnels* ni aux produits, services ou activités qui relèvent de la compétence ou de l'autorité des personnes suivantes : • le ministre de la Défense nationale; • le directeur du Service canadien du renseignement de sécurité; • le chef du Centre de la sécurité des télécommunications; • toute autre personne qui est responsable d'un ministère ou d'un organisme fédéral ou provincial et qui est désignée par règlement. <u>Section 2.5.3 – Exigences</u> Les exigences prévues en vertu de la Loi sur l'IA s'appliquent en lien avec les activités réglementées. Aux fins de l'application de la Loi sur l'IA « le traitement ou le fait de rendre disponibles des données liées à l'activité humaine afin de concevoir, de développer ou d'utiliser un système d'[IA] » et « la conception, le développement ou le fait de rendre disponible un système d'[IA] ou la gestion de son exploitation » dans le cadre des		

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	échanges ou du commerce internationaux ou interprovinciaux sont considérés comme des « activités réglementées » (art. 5). La personne qui, dans le cadre d'une activité réglementée, traite ou rend disponibles des données anonymisées, doit établir des mesures concernant la manière d'anonymiser ces données et l'utilisation ou la gestion des données anonymisées (art. 6). Conformément aux règlements, le responsable d'un système d'IA (la personne qui le conçoit, le développe ou le rend disponible) doit évaluer si ce système a une incidence élevée, c'est-à-dire si le système satisfait aux critères d'un système à incidence élevée établis par règlement. Dans l'affirmative, le responsable du système doit établir des mesures visant à cerner, évaluer et atténuer les risques de préjudice ou de résultats biaisés que pourrait entraîner l'utilisation de ce système. Il doit aussi établir des mesures visant à assurer le respect des mesures d'atténuation mises en place et à évaluer leur efficacité (art. 7 à 9).	Non divulgation des règles d'anonymisation des données et par le fait même du niveau d'incidence sur les individus et les organisations et identification impossible des préjudices associés	La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation des activités ci-contre en permettant l'identification des données devant être utilisées par chaque activité de gouvernance ainsi que les opérations d'anonymisation visées Et Les 10 outils de gestion de projet de PIGA-TI ainsi que les standards ISO applicables permettront de justifier, planifier, gérer et suivre la réalisation des bénéfices des projets reliés à l'arrivée des nouveaux systèmes et des versions futures Et La gestion de changement TI de PIGA-TI et les standards ISO applicables aideront à la définition des activités d'évolution des applications IA en place en considération des activités d'anonymisation utilisées Et Le plan de relève de PIGA-TI et les standards ISO applicables aideront à la sécurisation des systèmes et de leurs données, en

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
			considération des activités d'anonymisation utilisées, pour les sites de production et de relève exploités
Écosystème de l'intelligence artificielle du Canada - Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés	Afin de gérer et d'atténuer ces risques, les signataires du présent code s'engagent à adopter les mesures définies. Le code décrit les mesures qui devraient être appliquées en attendant l'adoption de règlements en application de la *Loi sur l'intelligence artificielle et les données* par toute entreprise qui développe ou gère les opérations d'un système d'IA génératif ayant des capacités générales. Il décrit aussi les mesures supplémentaires qui devraient être prises par toute entreprise qui développe ou gère les opérations d'un tel système rendu accessible à un vaste public, soit des systèmes dont l'éventail d'utilisations potentiellement nuisibles ou inappropriées est plus vaste. Les entreprises qui développent et gèrent des systèmes génératifs de pointe jouent des rôles importants et complémentaires. Les développeurs et les gestionnaires doivent coopérer pour veiller à ce que les répercussions négatives soient examinées par l'entreprise appropriée. Bien que le cadre décrit ici soit propre aux systèmes d'IA génératifs avancés, bon nombre des mesures peuvent être	Bien qu'ils présentent de nombreux avantages, les systèmes d'IA générative avancés comportent également un profil de risque qui est manifestement considérable. Cela s'explique par la vaste portée des données au moyen desquels ils sont entraînés, le large éventail d'utilisations potentielles des systèmes et l'ampleur de leur déploiement. Les systèmes qui sont accessibles au public pour un éventail d'utilisations peuvent présenter des risques pour la santé et la sécurité, propager des préjugés et avoir des répercussions sociétales plus vastes, particulièrement lorsqu'ils sont utilisés par des auteurs malveillants. Par exemple, la capacité de produire des images et des vidéos réalistes ou de se faire passer pour de vraies personnes peut permettre des tromperies d'une envergure qui peut nuire à d'importantes institutions, notamment aux systèmes de justice démocratique et pénale. Ces systèmes	La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation des activités ci-contre en permettant l'ajout d'activités du code de conduite à la gouvernance de l'entreprise afin de confirmer les exigences d'affaires et pour les systèmes qui seront à considérer

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	appliquées en grande partie à divers systèmes d'IA à incidence élevée et peuvent être facilement adaptées par les entreprises qui travaillent au sein de l'écosystème canadien d'IA. Il est également important de noter que les directives ne changent en rien les obligations juridiques que les entreprises peuvent avoir, par exemple, au titre de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Dans le cadre de cet engagement volontaire, les développeurs et les gestionnaires de systèmes génératifs avancés s'engagent à s'efforcer d'atteindre les résultats suivants : • **Responsabilisation** – Les entreprises comprennent leur rôle à l'égard des systèmes qu'elles développent ou gèrent, mettent en place des systèmes appropriés de	peuvent également avoir une incidence importante sur les droits individuels en matière de protection de la vie privée, comme le souligne la Déclaration sur l'IA générative des autorités de protection des données et de la vie privée du G7. Les organisations peuvent également adapter les systèmes génératifs pour des utilisations précises – comme les applications de gestion des connaissances organisationnelles ou les outils de service à la clientèle – qui présentent généralement un éventail plus restreint de risques. Malgré tout, les développeurs et les gestionnaires de tels systèmes devraient prendre un certain nombre de mesures pour veiller à ce que les risques soient bien cernés et atténués. Non-respect des exigences ci-contre	Les 10 outils de gestion de projet de PIGA-TI permettront de justifier, planifier, gérer et suivre la réalisation des bénéfices des

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	gestion des risques et collaborent avec d'autres entreprises au besoin pour éviter qu'il y ait des lacunes. • **Sécurité** – Des évaluations des risques doivent être réalisées pour les systèmes, et les mesures d'atténuation nécessaires doivent être prises avant le déploiement pour veiller à ce que l'exploitation des systèmes soit sécuritaire. • **Justice et équité** – L'incidence potentielle en matière de justice et d'équité est évaluée et gérée à différentes étapes de l'élaboration et du déploiement des systèmes. • **Transparence** – Suffisamment de renseignements sont publiés pour permettre aux consommateurs de prendre des décisions éclairées et aux experts d'évaluer si les risques ont été adéquatement gérés. • **Surveillance humaine** – L'utilisation du système est surveillée après le déploiement, et des mises à jour sont mises en œuvre au besoin pour gérer les risques qui se matérialisent. • **Validité et fiabilité** – Les systèmes fonctionnent comme prévu, sont sécurisés contre les cyberattaques, et leur comportement en réponse aux diverses tâches ou situations auxquelles ils sont susceptibles d'être exposés est compris.		projets reliés à l'arrivée des nouveaux systèmes et des versions futures Le plan de relève de PIGA-TI et les standards ISO applicables aideront à la sécurisation des systèmes et de leurs données, en considération des activités d'anonymisation utilisées, pour les sites de production et de relève exploités La gouvernance globale de PIGA-TI et les standards ISO applicables aideront à la réalisation des activités ci-contre en permettant de conserver les informations nécessaires aux décisions des consommateurs et des experts La gestion de changement TI de PIGA-TI et les standards ISO applicables aideront à la définition des activités d'évolution des applications IA en place Le plan de relève de PIGA-TI et les standards ISO applicables aideront à la sécurisation des systèmes et de leurs données, en considération des activités d'anonymisation utilisées,

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	Les signataires s'engagent également à soutenir le développement continu d'un écosystème d'IA fiable et responsable au Canada. Notamment, la contribution à l'élaboration et à l'application de normes, la transmission d'information et de pratiques exemplaires à d'autres membres de l'écosystème de l'IA, la collaboration avec des chercheurs qui travaillent pour l'avancement de l'IA responsable et la collaboration avec d'autres intervenants, y compris les gouvernements, pour appuyer la sensibilisation et l'éducation du public à l'égard de l'IA. Les signataires s'engagent également à élaborer et à déployer des systèmes d'IA de manière à favoriser une croissance axée sur l'inclusion et la durabilité au Canada, notamment en accordant la priorité aux droits de la personne, à l'accessibilité et à la durabilité environnementale, et à exploiter le potentiel de l'IA pour relever les défis mondiaux les plus urgents de notre époque.	Non-respect des exigences ci-contre	pour les sites de production et de relève exploités Et La gestion de changement TI de PIGA-TI et les standards ISO applicables aideront à la définition des activités d'évolution des applications IA en place La gouvernance globale de PIGA-TI et les standards ISO applicables pourront aider à la réalisation des activités ci-contre

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
ISO/ IEC 27017	L'ISO/CEI 27017:2015 fournit des lignes directrices pour les contrôles de sécurité de l'information applicables à la fourniture et à l'utilisation de services cloud en fournissant : - des lignes directrices supplémentaires pour la mise en œuvre des contrôles pertinents spécifiés dans l'ISO/IEC 27002 ; - Contrôles supplémentaires avec des conseils de mise en œuvre qui se rapportent spécifiquement aux services cloud. La présente Recommandation | La Norme internationale fournit des contrôles et des conseils de mise en œuvre pour les fournisseurs de services cloud et les clients de services cloud	En fonction des risques identifiés	Utilisations à confirmer pour les lois et règlements précédents
ISO/ IEC 27001	ISO/IEC 27001 est la norme la plus connue au monde pour les systèmes de management de la sécurité de l'information (SMSI). Il définit les exigences auxquelles un SMSI doit répondre. La norme ISO/IEC 27001 fournit aux entreprises de toutes tailles et de tous secteurs d'activité des orientations pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un système de management de la sécurité de l'information. La conformité à la norme ISO/IEC 27001 signifie qu'une organisation ou une entreprise a	En fonction des risques identifiés	Utilisations à confirmer pour les lois et règlements précédents

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
	mis en place un système de gestion des risques liés à la sécurité des données détenues ou traitées par l'entreprise, et que ce système respecte toutes les meilleures pratiques et principes inscrits dans la présente Norme internationale.		
ISO/ IEC 27002	ISO/IEC 27002 est une norme internationale qui fournit des conseils aux organisations qui cherchent à établir, mettre en œuvre et améliorer un système de gestion de la sécurité de l'information (SMSI) axé sur la cybersécurité. Alors que la norme ISO/IEC 27001 définit les exigences d'un SMSI, la norme ISO/IEC 27002 propose des bonnes pratiques et des objectifs de contrôle liés aux principaux aspects de la cybersécurité, notamment le contrôle d'accès, la cryptographie, la sécurité des ressources humaines et la réponse aux incidents. La norme sert de modèle pratique pour les organisations qui souhaitent protéger efficacement leurs actifs informationnels contre les cybermenaces. En suivant les lignes directrices ISO/IEC 27002, les entreprises peuvent adopter une approche proactive de la gestion des risques de cybersécurité et protéger les informations critiques contre les accès non autorisés et les pertes.	En fonction des risques identifiés	Utilisations à confirmer pour les lois et règlements précédents

Lois/ Règlements/ Standards applicables (ISO – Information Security)	Activités/ livrables à réaliser (obligations)	Risques relies au statut quo (non réalisation et/ ou non-respect)	Outils de PIGA-TI pouvant être mis à profit lors de la réalisation des activités/ livrables (obligations)
ISO/ IEC 27005	Ce document fournit des conseils pour aider les organisations à : — satisfaire aux exigences de l'ISO/CEI 27001 concernant les actions visant à faire face aux risques liés à la sécurité de l'information ; — effectuer des activités de gestion des risques liés à la sécurité de l'information, en particulier l'évaluation et le traitement des risques liés à la sécurité de l'information. Le présent document s'applique à tous les organismes, quels que soient leur type, leur taille ou leur secteur.	En fonction des risques identifiés	Utilisations à confirmer pour les lois et règlements précédents