

Cadre de Gouvernance de l'IA Générative

Exploitez la puissance de l'intelligence artificielle générative (IA Gen) et gérez correctement les risques.



Auteurs



Scott A. Emett, PhD

Associate Professor, Arizona State University



Marc Eulerich, PhD, CIA

Dean and Professor, University of Duisburg-Essen



Jason Pikoos

Managing Partner, Connor Group



David A. Wood, PhD

Professor, Brigham Young University

Préface

Nous sommes reconnaissants envers les plus de 1000 examinateurs, contributeurs, endosseurs et sponsors de cette entreprise colossale. Construire des modèles de gouvernance appropriés pour des technologies perturbatrices et en évolution rapide nécessite de prendre en compte de nombreux points de vue. Ainsi, nous avons impliqué des leaders d'opinion et des experts en processus provenant de l'industrie, du milieu universitaire et des organismes de réglementation.

Contenu

Introduction	04
Aperçu du Cadre de Gouvernance de l'IA Générative	05
Comment utiliser le cadre	06
Principales Considérations de Contrôle pour Atténuer les Risques de l'IA	10
Alignement Stratégique et Environnement de Contrôle	10
Gestion des Données et Conformité	11
Gestion Opérationnelle et Technologique	12
Considérations humaines, éthiques et sociales	14
Transparence, responsabilité et amélioration continue	17

Introduction

Ce cadre vise à aider les organisations à exploiter la puissance de l'intelligence artificielle générative (IA générative) tout en gérant adéquatement ses risques. Plus de 1000 praticiens et universitaires ont contribué au développement de ce cadre. Les experts participants comprennent des spécialistes de l'IA, des auditeurs internes et externes, des régulateurs, des membres de comités d'audit, des dirigeants et autres. Nous avons élaboré ce cadre pour bénéficier aux organisations de divers secteurs, y compris à but lucratif, non lucratif, gouvernemental et plus encore.

La « IA générative » repousse les limites de la gouvernance en créant des informations entièrement nouvelles qui n'existaient pas auparavant. Elle introduit ainsi une multitude de nouvelles possibilités et de risques que les organisations doivent affronter.

Bien que les individus utilisent fréquemment la IA générative directement via des produits achetés comme ChatGPT d'OpenAI ou Gemini de Google, ils peuvent également y avoir recours sans le savoir. Par exemple, les employés peuvent utiliser involontairement la IA générative via des programmes logiciels contenant des composants IA générative intégrés, tels que Copilot de Microsoft. De plus, la IA générative peut être intégrée dans des solutions d'IA spécifiques à l'organisation comme un « GPT d'entreprise ». Ce cadre vise à aider dans chacune de ces situations en identifiant et en atténuant les risques liés à la IA générative.

Appuis

« Nous nous trouvons à une époque nouvelle et passionnante en ce qui concerne l'IA et ses effets actuels et potentiels sur la société et les entreprises. Conceptualiser une approche cohérente pour les organisations en matière de gouvernance de l'IA dans cet environnement en rapide évolution devient crucial. Je considère cet effort comme une étape significative et importante dans ce domaine vital, et je félicite les auteurs en tant que précurseurs perspicaces ! »

Douglas F. Prawitt, PhD, CPA – Directeur de l'École de Comptabilité de l'Université Brigham Young et Directeur Principal du Conseil de COSO

« Le cadre de gouvernance de l'IA présente une approche fantastique pour les auditeurs internes, mais aussi pour d'autres prestataires d'assurance et le conseil d'administration afin de créer et valider une structure de gouvernance de l'IA efficace. »

Dorothea Mertmann – PDG de l'IIA Allemagne (Deutsches Institut für Interne Revision e.V.)

« Nous rencontrerons bientôt l'IA générative dans de nombreuses parties de notre vie professionnelle quotidienne. Avec ce cadre, l'audit interne peut traiter les risques à un stade précoce. Il peut sensibiliser les parties auditées et les soutenir dans la mise en place d'une gouvernance et d'un environnement de contrôle appropriés. De ce point de vue, le cadre de gouvernance de l'IA générative est un outil idéal pour positionner l'audit interne comme un point de contact fiable pour les risques associés à l'utilisation de l'intelligence artificielle. »

Gabrielle Rudolf von Rohr – Présidente, IIA Suisse

« Une adoption efficace de l'IA sera un avantage compétitif majeur, mais beaucoup ne savent pas par où commencer et comment l'appliquer. Quelques outils d'IA existent maintenant avec beaucoup d'autres à venir, et ils arrivent rapidement. Avoir une stratégie d'adoption de l'IA intelligente avec des contrôles, des données et des processus sous-jacents prêts pour l'IA prend du temps. Les entreprises les plus compétitives font ces choses maintenant. »

Jeff Pickett – Président, Connor Group

« Chez Boomi, nous comprenons le pouvoir de la clarté et de l'action. Ce cadre de gouvernance de l'IA, que j'ai eu le privilège de contribuer à façonner, incarne cela en fournissant un résumé d'une page idéal pour les discussions en salle de conseil, ainsi qu'une répartition détaillée des contrôles pour une mise en œuvre pratique. Il est conçu non seulement pour être adopté, mais aussi pour être adapté, permettant aux entreprises d'évaluer leur conformité et leur maturité, en identifiant les domaines de force et les opportunités d'amélioration. Nous sommes fiers d'être parmi les premiers à mettre en œuvre et à promouvoir un outil qui comble si efficacement le fossé entre la surveillance stratégique et l'excellence opérationnelle. »

Waseem Samaan, CPA, CIA – Directeur de l'audit et des risques chez Boomi

Le Cadre de Gouvernance de l'IA Générative catégorise la gouvernance de la IA générative en cinq domaines essentiels.

1. Alignement Stratégique et Environnement de Contrôle
2. Gestion des Données et Conformité
3. Gestion Opérationnelle et Technologique
4. Considérations Humaines, Éthiques et Sociales
5. Transparence, Responsabilité et Amélioration Continue

Cadre Conceptuel de gouvernance en IA générative

Gestion des opérations et de la technologie

- Intégrer l'IA dans les processus opérationnels.
- Gérer la technologie de l'IA et la sécurité informatique.

Gestion des données et de la conformité

- Mettre en place des processus d'identification, d'évaluation et d'atténuation des risques liés aux données.
- Veiller au respect des normes juridiques et réglementaires.



Transparence, responsabilité et amélioration continue

- Garantir la transparence et la traçabilité du processus décisionnel en matière d'IA.
- Suivre l'évolution de l'IA et mettre à jour les pratiques de gouvernance.

Considérations humaines, éthiques et sociales

- Organiser des formations à l'IA et gérer les risques liés aux ressources humaines.
- Garantir une utilisation éthique de l'IA qui atténue les préjugés.
- Évaluer et gérer les impacts sociaux et de réputation.
- Évaluer et gérer les incidences sur l'environnement.

Dans chacun de ces domaines, le cadre identifie plusieurs risques et considérations de contrôle. En délimitant les risques et les considérations de contrôle, le cadre aide les organisations (1) à comprendre comment l'IA générative peut menacer les objectifs organisationnels et (2) à élaborer des approches de gouvernance qui atténuent ces risques. Nous fournissons l'ensemble complet des risques et considérations de contrôle à la fin de ce document.

Ce cadre devrait aider les organisations à atteindre les objectifs suivants :

- Améliorer la gestion globale des risques liés à l'IA générative
- Établir des structures de gouvernance pour l'IA générative
- Stimuler l'amélioration stratégique et la conformité
- Assurer l'engagement et la confiance des parties prenantes
- Établir une référence pour l'amélioration continue

Comment utiliser le cadre

Avant d'utiliser le cadre, les organisations doivent considérer leur appétit et leur tolérance au risque dans le contexte de la IA générative. Comme pour toute autre technologie, une organisation doit décider combien de risques elle est prête à accepter lors de l'adoption d'applications et de solutions IA générative. Ce cadre guide les organisations dans l'alignement des risques liés à la IA générative avec leur appétit pour le risque établi. Nous recommandons aux organisations d'adopter le cadre en quatre étapes.

ÉTAPE 01

Définir les objectifs et les buts de la IA générative

Définir des objectifs et des buts spécifiques pour la IA générative. S'assurer que ces objectifs et buts sont alignés avec :

- La stratégie d'entreprise établie et les objectifs de digitalisation
- Les attentes des parties prenantes
- Les exigences de conformité et réglementaires
- Les contraintes budgétaires

ÉTAPE 02

Établir la portée appropriée du cadre pour votre organisation

Le Cadre de Gouvernance de l'IA Générative vise à servir une variété d'organisations; certains des domaines, risques et considérations de contrôle du cadre peuvent ne pas s'appliquer à votre organisation. Les organisations doivent aligner la portée du cadre avec leurs besoins et priorités organisationnels :

- Identifier les domaines prioritaires du cadre de gouvernance pour votre organisation
- Identifier les principaux risques dans chaque domaine les plus pertinents pour votre organisation
- Déterminer les fonctions au sein de votre organisation les plus impactées par les risques liés à la IA générative (par exemple, département, unité d'affaires)
- Identifier les processus, projets et technologies les plus exposés aux risques liés à la IA générative
- Sélectionner les parties prenantes appropriées à impliquer dans la gouvernance de la IA générative

ÉTAPE 03

Compléter une évaluation des risques de gouvernance de l'IA

Nous recommandons une approche en cinq étapes pour l'évaluation des risques de la IA générative avec un livrable produit à chaque étape. L'identification initiale des risques et l'évaluation de la IA générative dans votre organisation peuvent suivre les procédures d'évaluation des risques traditionnelles présentées dans la figure. Nous fournissons des détails supplémentaires et un sondage qui vous permet de réaliser une évaluation détaillée de la maturité de la gouvernance de la IA générative avec un benchmarking au lien suivant : [genai.global](#).

Planification et préparation	<ul style="list-style-type: none"> • Développer les objectifs et la portée avec le commanditaire du projet • Identifier les parties prenantes et organiser un lancement • Recueillir la documentation et compléter l'enquête • Confirmer les échéances et planifier les réunions 	LIVRABLE : Lancement du projet et plan
Collecte et examen des données	<ul style="list-style-type: none"> • Revoir les résultats de l'enquête et la documentation pertinente (par exemple, les politiques et les documents stratégiques) • Organiser un atelier avec les cadres supérieurs en finance, comptabilité et TI 	LIVRABLE : Résultats de l'enquête et benchmarking
Évaluation et priorisation des risques	<ul style="list-style-type: none"> • Comparer le paysage actuel de l'IA de l'organisation avec le cadre de gouvernance de l'IA • Identifier les risques non atténués • Prioriser les risques à l'aide de l'enquête et des sessions de travail 	LIVRABLE : Résumé des risques non atténués priorisés
Recommandations et feuille de route	<ul style="list-style-type: none"> • Proposer des stratégies de mitigation actionnables pour les risques non atténués prioritaires • Développer une feuille de route et un calendrier de mise en œuvre 	LIVRABLE : Recommandations priorisées et feuille de route
Résultats publiés	<ul style="list-style-type: none"> • Préparer un rapport sommaire exécutif • Revoir avec les parties prenantes clés en finance, comptabilité et TI • Aligner les plans d'avenir et les prochaines étapes 	LIVRABLE : Rapport exécutif final

ÉTAPE 04

Exécuter votre plan défini (basé sur votre évaluation des risques)

Dans l'étape 4, les organisations intègrent le plan de gouvernance de l'IA dans leurs plans stratégiques selon les risques identifiés. Une gouvernance efficace nécessite d'adapter les méthodes et ressources existantes pour soutenir les risques uniques et les considérations de contrôle des projets d'IA. Nous recommandons aux organisations de traiter la gouvernance et les contrôles de l'IA comme une priorité critique compte tenu de leur importance émergente et de leurs risques uniques.

Conclusion

Ce cadre vise à aider les organisations à créer une structure de gouvernance efficace et efficiente pour IA générative. Il a été vérifié et préparé par de nombreux groupes et professionnels.

Vous trouverez dans les pages suivantes l'intégralité du cadre de gouvernance, y compris les risques et les considérations de contrôle. Le cadre est fourni comme une ressource gratuite. Pour compléter le cadre, nous avons développé un modèle de maturité et des services de benchmarking. Vous pouvez en savoir plus à ce sujet au genai.global. Le cadre n'est pas conçu pour traiter tous les risques liés aux données et à la technologie et nous recommandons donc qu'il soit utilisé en conjonction avec d'autres cadres de gouvernance existants comme le Cadre de Contrôle Interne Intégré COSO, le Cadre de Gestion des Risques d'Entreprise COSO, COBIT et le Modèle des Trois Lignes.

Enfin, nous nous attendons à ce que ce cadre évolue au fur et à mesure que la technologie IA générative continue d'évoluer et de s'étendre. En tant que tel, les auteurs avec l'aide des organisations sponsors fourniront des mises à jour au fur et à mesure que des changements se produisent.

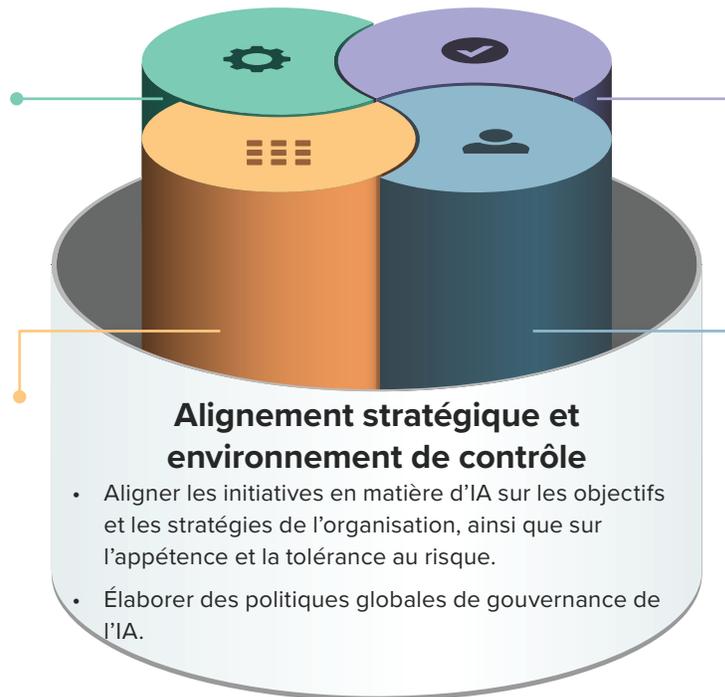
Cadre Conceptuel de gouvernance en IA générative

Gestion des opérations et de la technologie

- Intégrer l'IA dans les processus opérationnels.
- Gérer la technologie de l'IA et la sécurité informatique.

Gestion des données et de la conformité

- Mettre en place des processus d'identification, d'évaluation et d'atténuation des risques liés aux données.
- Veiller au respect des normes juridiques et réglementaires.



Transparence, responsabilité et amélioration continue

- Garantir la transparence et la traçabilité du processus décisionnel en matière d'IA.
- Suivre l'évolution de l'IA et mettre à jour les pratiques de gouvernance.

Considérations humaines, éthiques et sociales

- Organiser des formations à l'IA et gérer les risques liés aux ressources humaines.
- Garantir une utilisation éthique de l'IA qui atténue les préjugés.
- Évaluer et gérer les impacts sociaux et de réputation.
- Évaluer et gérer les incidences sur l'environnement.

DOMAIN	DESCRIPTION	OBJECTIFS CLÉS	PRINCIPAUX RISQUES ADRESSÉS
Alignement Stratégique et Environnement de Contrôle	Ce domaine se concentre sur la garantie que les initiatives en matière d'IA sont en harmonie avec les objectifs globaux et les stratégies de l'organisation. Cela implique de définir l'appétit et la direction pour l'utilisation de l'IA et d'établir l'environnement de contrôle autour de l'utilisation de l'IA.	<ul style="list-style-type: none"> • Aligner les initiatives en matière d'IA avec les objectifs, stratégies et appétit/tolérance aux risques de l'organisation. • Développer des politiques complètes de gouvernance de l'IA. 	<ul style="list-style-type: none"> • Risques Stratégiques et de Planification • Risques de l'Environnement de Contrôle
Gestion des Données et de la Conformité	Ce domaine se concentre sur l'identification, l'évaluation et l'atténuation des risques liés aux données ; et sur la garantie de la conformité à toutes les normes légales et réglementaires pertinentes.	<ul style="list-style-type: none"> • Établir des processus pour identifier, évaluer et atténuer les risques liés aux données. • Assurer la conformité aux normes légales et réglementaires. 	<ul style="list-style-type: none"> • Risques Liés aux Données • Risques du Régime Légal et Réglementaire
Gestion Opérationnelle et Technologique	Ce domaine se concentre sur l'intégration de l'IA dans les processus d'affaires, la gestion de la technologie elle-même et la garantie de la sécurité informatique. Il aborde l'application pratique de l'IA dans les opérations quotidiennes.	<ul style="list-style-type: none"> • Intégrer l'IA dans les processus opérationnels. • Gérer la technologie de l'IA et la sécurité informatique. 	<ul style="list-style-type: none"> • Risques de Gestion des Processus • Risques d'Évaluation et de Sélection Technologique • Risques Accrus de Sécurité Opérationnelle et Informatique
Considérations Humaines, Éthiques et Sociales	Ce domaine aborde l'impact de l'IA sur la main-d'œuvre, les considérations éthiques et les implications sociales plus larges. Il souligne l'importance de traiter les aspects centrés sur l'humain du déploiement de l'IA.	<ul style="list-style-type: none"> • Conduire la formation en IA et gérer les risques liés aux ressources humaines. • Assurer une utilisation éthique de l'IA qui atténue les biais. • Évaluer et gérer les impacts réputationnels et sociaux. • Évaluer et gérer les impacts environnementaux. 	<ul style="list-style-type: none"> • Risques de Connaissance et de Formation • Risques de Ressources Humaines et d'Emploi • Risques Éthiques et de Biais • Risques de Réputation et Sociaux • Risques ESG
Transparence, Responsabilité et Amélioration Continue	Ce domaine se concentre sur la garantie que l'utilisation de l'IA dans la prise de décision est transparente et responsable. Il se concentre également sur l'amélioration continue des pratiques de gouvernance de l'IA, en s'adaptant aux nouveaux défis et technologies.	<ul style="list-style-type: none"> • Assurer une prise de décision en IA transparente et traçable. • Surveiller l'évolution de l'IA et mettre à jour les pratiques de gouvernance. 	<ul style="list-style-type: none"> • Risques de Transparence, de Traçabilité et de Confiance • Évolution Continue des Risques Technologiques • Risques Divers • Risques Hautement Conceptuels ou Hypothétiques

Principales Considérations de Contrôle pour Atténuer les Risques de l'IA

Alignement Stratégique et Environnement de Contrôle

Considérations de Contrôle pour les Risques Stratégiques et de Planification

RISQUES	
<p>Cette catégorie de risques aborde les risques de ne pas aligner les initiatives en matière d'IA avec les objectifs organisationnels à long terme.</p>	
CONSIDÉRATIONS DE CONTRÔLE	
Cadre de Gestion des Risques liés à l'IA	Développer un cadre pour la gouvernance des risques liés à l'IA. Ce cadre devrait s'intégrer à d'autres cadres ou les mettre à jour (par exemple, le cadre de contrôle interne intégré du CO-SO, le cadre de gestion des risques d'entreprise du COSO, COBIT).
Feuille de Route Stratégique pour l'IA	Élaborer une feuille de route stratégique avec l'adhésion des différentes fonctions pour l'intégration de l'IA, en accord avec les objectifs organisationnels.
Revue Stratégique Régulière	Établir un processus de révision régulier pour aligner les initiatives en matière d'IA avec les stratégies organisationnelles en évolution.
Engagement des Parties Prenantes	Impliquer les principales parties prenantes dans la planification des projets d'IA pour assurer l'alignement avec les objectifs commerciaux et l'appétit pour le risque.
Suivi de la Performance	Mettre en place des métriques et des indicateurs clés de performance (KPI) pour mesurer l'efficacité des initiatives en matière d'IA dans l'atteinte des objectifs stratégiques. Surveiller également les évolutions des capacités de l'IA pour confirmer qu'elles continuent de s'aligner avec les objectifs stratégiques.
Planification de Contingence	Développer des plans de contingence pour les projets d'IA afin de gérer les résultats inattendus ou les changements de direction stratégique.
Planification de Scénarios et Prévisions	Mettre en œuvre la planification de scénarios pour les initiatives en matière d'IA afin d'anticiper et de se préparer aux événements imprévus.

Principales Considérations de Contrôle pour Atténuer les Risques de l'IA

Alignement Stratégique et Environnement de Contrôle

Considérations de Contrôle pour les Risques de l'Environnement de Contrôle

RISQUES	
<p>Cette catégorie de risques aborde la nécessité de développer des politiques nouvelles ou mises à jour, d'éduquer les utilisateurs sur la gestion de l'IA, de structurer les responsabilités au sein de la gouvernance de l'IA, et de gérer la responsabilité résiduelle des décideurs qui se fient aux recommandations de l'IA.</p>	
CONSIDÉRATIONS DE CONTRÔLE	
Développement de Politiques et Gouvernance	Superviser des politiques complètes de gouvernance et d'utilisation de l'IA basées sur l'appétit pour le risque, la stratégie, et les directives légales pertinentes.
Rôles et Responsabilités définis	Définir et communiquer les rôles et responsabilités liés à la gouvernance de l'IA au sein de l'organisation.
Établir un Comité de Gouvernance de l'IA	Établir un comité ou une institution comparable pour superviser la gouvernance et la mise en œuvre des politiques de l'IA. Le comité doit avoir une représentation large à la fois verticalement et horizontalement dans l'organisation pour intégrer tous les aspects nécessaires de l'utilisation de l'IA générative.
Inventaire de l'IA	Assurer la tenue d'un inventaire centralisé de tous les cas d'utilisation de l'IA générative en développement ou en production dans l'organisation.
Revue et Mise à Jour Régulières des Politiques	S'assurer que les politiques de l'IA sont régulièrement revues et mises à jour pour refléter les nouveaux développements et connaissances.
Cadre Éthique pour l'IA	Mettre en œuvre un cadre éthique pour l'IA afin de guider la prise de décision dans les projets d'IA.
Plan de Réponse aux Incidents	Développer un plan de réponse aux incidents spécifiquement pour les problèmes liés à l'IA (par exemple, les violations de sécurité, les décisions d'affaires incorrectes).

Gestion des Données et Conformité

Considérations relatives au contrôle des risques liés aux données

RISQUES

Cette catégorie de risques concerne les risques liés aux violations de données, à l'accès non autorisé, à la mauvaise gestion, à la propagation d'informations incorrectes par les systèmes d'IA, à la dépendance excessive à l'égard de l'IA (dépendance à l'égard de l'IA) et à la menace des concurrents qui utilisent l'IA pour recueillir des renseignements.

CONSIDÉRATIONS DE CONTRÔLE

Cadre de gouvernance des données	Établir un cadre complet de gouvernance des données pour gérer les risques tels que la collecte, le stockage, l'accessibilité, la qualité, la confidentialité, la conservation, la sécurité, la suppression, l'exportation, etc. des données. Réviser et mettre à jour fréquemment.
Politiques de contrôle d'accès	Mettre en œuvre des politiques strictes de contrôle d'accès, y compris un accès basé sur les rôles, pour les outils et les données sensibles.
Chiffrement et anonymisation des données	Utiliser des techniques de chiffrement et d'anonymisation des données pour protéger les informations sensibles.
Outils de lignage des données d'IA	Suivre le lignage des données dans l'ensemble de l'organisation pour garantir la transparence de l'utilisation des données par les systèmes d'IA.
Audits réguliers des données	Effectuez des audits réguliers pour garantir l'intégrité des données et détecter tout accès non autorisé ou toute violation.
Modèles d'auto-apprentissage	Établir un processus d'audit et de surveillance clair pour les modèles d'auto-apprentissage afin de traiter les risques dès que possible. Les modèles d'auto-apprentissage sont des systèmes d'IA qui améliorent de manière autonome leurs performances et s'adaptent au fil du temps en apprenant à partir de nouvelles données et expériences sans instruction humaine explicite.

Considérations relatives au contrôle des risques juridiques et réglementaires

RISQUES

Cette catégorie de risques concerne les risques associés à la conformité aux lois changeantes et aux mandats gouvernementaux spécifiques à l'IA, y compris l'adaptation aux contraintes réglementaires, le respect des exigences en matière de transparence et de rapports, et la gestion des responsabilités juridiques liées aux actions de l'IA. Il s'agit également de se tenir au courant des normes juridiques internationales, de protéger la propriété intellectuelle et d'élaborer des stratégies d'engagement avec les organismes de réglementation et de réaction rapide aux changements juridiques.

CONSIDÉRATIONS DE CONTRÔLE

Processus de documentation et de déclaration	Maintenir une documentation et un reporting complets pour garantir la transparence et faciliter la conformité pour toutes les solutions d'IA dans l'organisation.
Contrôle de la conformité	Mettre en œuvre un processus de contrôle continu et de conformité aux lois et réglementations pertinentes.
Évaluation des risques juridiques liés à l'IA	Effectuer régulièrement des évaluations des risques juridiques pour les initiatives d'IA.
Surveillance et formation sur les changements réglementaires	Surveiller, mettre à jour et former régulièrement le personnel sur les nouveaux développements réglementaires affectant l'IA.
Stratégie de conformité transfrontalière	Élaborer des stratégies pour gérer la conformité dans différentes juridictions, en particulier dans le cadre d'opérations multinationales.

Gestion Opérationnelle et Technologique

Considérations relatives au contrôle des risques liés à la gestion des processus

RISQUES	
Cette catégorie de risques concerne l'utilisation opérationnelle de l'IA, y compris les risques liés à la validation des applications et des résultats de l'IA.	
CONSIDÉRATIONS DE CONTRÔLE	
Procédures opérationnelles normalisées pour l'utilisation de l'IA	Élaborer et mettre en œuvre des procédures opérationnelles normalisées (POS) pour les applications de l'IA dans le cadre des processus opérationnels.
Surveillance et contrôle des performances de l'IA	Établir des processus réguliers et récurrents pour évaluer les performances des applications de l'IA.
Protocoles de validation et de test	Mettre en œuvre des protocoles rigoureux de validation et de test avec l'approbation des parties prenantes pour les applications d'IA avant leur déploiement.
Procédures de gestion du changement	Élaborer des procédures de gestion du changement pour la mise en œuvre de l'IA afin de minimiser les perturbations opérationnelles.

Considérations relatives au contrôle des risques liés à l'évaluation et à la sélection des technologies

RISQUES	
Cette catégorie de risques concerne le processus de sélection des technologies d'IA qui répondent aux besoins de l'organisation.	
CONSIDÉRATIONS DE CONTRÔLE	
Cadre d'évaluation des technologies	Créer un cadre pour l'évaluation et la sélection des technologies d'IA qui correspondent aux objectifs et aux besoins de l'organisation, ainsi qu'aux exigences de conformité (sécurité, confidentialité, contrôles).
Évaluation des risques liés aux fournisseurs	Procéder à des évaluations approfondies des risques liés aux fournisseurs et à leurs solutions d'IA avant la mise en œuvre. Intégrer l'examen de l'IA dans les processus de gestion des risques des tiers et d'intégration des fournisseurs.
Protocole d'intégration et de gestion des fonctionnalités d'IA	Établir un protocole d'approbation, d'intégration et de gestion des nouvelles fonctionnalités d'IA dans les systèmes existants. Ce protocole devrait comprendre un processus d'évaluation complet
Examen postérieur à la mise en œuvre	Effectuer des examens postérieurs à la mise en œuvre afin d'évaluer l'efficacité et l'impact de la technologie de l'IA.

Operational and Technology Management

Considérations sur les risques de sécurité et d'accès opérationnels et informatiques améliorés

RISQUES

Cette catégorie de risque aborde la nécessité de maintenir la confidentialité des données, de sécuriser les systèmes d'IA contre les menaces, de gérer les risques de transfert de données et de répondre aux menaces de cybersécurité telles que l'ingénierie sociale par l'IA.

CONSIDÉRATIONS DE CONTRÔLE

Politiques de sécurité informa-tique robustes	Assurer que les systèmes d'IA respectent les autres politiques organisationnelles. Au besoin, rédiger des compléments de politique/procédure pour combler les lacunes posées par le sys-tème d'IA.
Formation à la sécurité des don-nées pour les employés	Fournir une formation complète sur la sécurité des données aux employés impliqués dans les opérations d'IA.
Plans de réponse aux incidents et de récupération	Établir des plans de réponse aux incidents et de récupération pour les potentielles violations de sécurité ou les défaillances opérationnelles majeures des systèmes d'IA clés.
Gestion des accès et authentifica-tion	Renforcer les mécanismes de gestion des accès et d'authentification pour les systèmes d'IA et les systèmes connectés à ceux-ci. Évaluer l'accès de l'IA à tous les systèmes.
Surveillance continue des me-naces de sécurité	Maintenir des systèmes de surveillance continue pour détecter et répondre rapidement aux menaces de sécurité.

Considérations humaines, éthiques et sociales

Considérations sur les contrôles des risques liés aux connaissances et à la formation

RISQUES	
Cette catégorie de risque aborde la nécessité de former les utilisateurs sur les risques et les limitations de l'IA générative.	
CONSIDÉRATIONS DE CONTRÔLE	
Communiquer de manière transparente la date des dernières données incluses dans le modèle d'IA	Assurez-vous que les utilisateurs sont conscients de l'actualité des informations dans le modèle par rapport à l'organisation et au monde.
Plan de formation pour les employés	Développez un plan de formation pour enseigner aux employés comment utiliser les modèles d'IA, les limitations potentielles des modèles d'IA, et les autres risques liés à l'utilisation de l'IA.

Considérations sur les contrôles des risques liés aux ressources humaines et à l'emploi

RISQUES	
This risk category addresses the risks associated with human resources, such as the impact of GenAI on employment rates, the potential replacement of jobs by GenAI in certain sectors, and the fear among personnel of job loss due to GenAI implementation.	
CONSIDÉRATIONS DE CONTRÔLE	
Stratégie de communication transparente	Développez une stratégie de communication transparente sur l'impact de l'IA sur les emplois et les rôles.
Stratégies de création d'emplois liés à l'IA	Identifiez et développez de nouveaux rôles et opportunités d'emploi créés par les avancées de l'IA.
Implication des employés dans la mise en œuvre de l'IA	Impliquez les employés dans la conception et la mise en œuvre des solutions d'IA pour favoriser l'acceptation et la compréhension.
Programmes de requalification et de perfectionnement	Mettez en œuvre des programmes pour requalifier et perfectionner les employés affectés par l'intégration de l'IA.
Boucles de rétroaction sur l'intégration de l'IA	Créez des mécanismes de rétroaction pour que les employés puissent exprimer leurs préoccupations et suggestions concernant l'intégration de l'IA.

Considérations humaines, éthiques et sociales

Considérations sur les contrôles des risques éthiques et de biais

RISQUES

Cette catégorie de risque aborde les risques que les systèmes d'IA perpétuent des biais ou soient utilisés de manière non éthique.

CONSIDÉRATIONS DE CONTRÔLE

Cadre de détection et d'atténuation des biais	Développer et mettre en œuvre un cadre pour l'identification et l'atténuation des biais dans les systèmes d'IA.
Données diversifiées	Assurer la diversité des ensembles de données pour entraîner l'IA afin de réduire le risque de biais inhérents.
Formation régulière à l'éthique	Organiser régulièrement des formations pour les équipes utilisant et gérant l'IA sur les considérations éthiques et la sensibilisation aux biais.
Mécanismes de retour d'information des utilisateurs	Mettre en place des mécanismes pour recevoir et traiter les retours d'information des utilisateurs.
Audits de conformité éthique par des tiers	Effectuer des audits et/ou examiner les rapports d'audit et les contrôles des outils d'IA achetés auprès de parties externes.

Considérations sur les contrôles des risques de réputation et sociaux

RISQUES

Cette catégorie de risque aborde les risques liés aux dommages de réputation dus à la communication basée sur l'IA.

CONSIDÉRATIONS DE CONTRÔLE

Mise en œuvre de politiques de « l'humain au milieu » pour les divulgations sensibles	Pour les divulgations jugées importantes ou sensibles, exiger que tout le contenu généré par l'IA soit examiné par un ou plusieurs humains avant d'être publié.
Équipe de réponse à la réputation	Désigner et former un groupe de personnes sur la manière de répondre en cas de réaction négative au contenu généré par l'IA.

Considérations humaines, éthiques et sociales

Considérations sur les contrôles des risques ESG

RISQUES

Cette catégorie de risque aborde les risques associés à l'impact environnemental des systèmes d'IA, les implications sociales telles que le déplacement de la main-d'œuvre ou la perturbation sociétale, et les défis de gouvernance.

CONSIDÉRATIONS DE CONTRÔLE

Cadre de gouvernance pour l'impact environnemental, social et de gouvernance	Utiliser et modifier le cadre ESG existant pour gérer l'impact ESG de l'IA.
Évaluations de l'impact environnemental pour l'IA	Évaluer l'impact environnemental des systèmes d'IA (par exemple, la consommation d'énergie).
Évaluation de l'impact social pour l'IA	Évaluer les impacts potentiellement non éthiques et/ou indésirables (voir aussi les contrôles des risques éthiques et de biais).
Évaluation de l'impact de la gouvernance pour l'IA	Évaluer les impacts potentiels sur les autres fonctions de gouvernance et d'assurance.
Pratiques de développement d'IA durable	Adopter des pratiques respectueuses de l'environnement dans le développement et le déploiement de l'IA.
Formation ESG pour les équipes d'IA	Fournir une formation sur les considérations ESG pour les équipes impliquées dans le développement et les opérations de l'IA.

Transparence, responsabilité et amélioration continue

Considérations sur les contrôles des risques de transparence, de traçabilité et de confiance

RISQUES

Cette catégorie de risque aborde la nécessité de clarté dans les processus de prise de décision de l'IA, d'assurer la traçabilité des résultats et des décisions, et de réduire le risque de surestimation ou de biais d'autorité où le jugement de l'IA est accepté sans suffisamment de vérifications.

CONSIDÉRATIONS DE CONTRÔLE

Documentation de la prise de décision de l'IA	Mettre en œuvre des exigences pour documenter l'utilisation et les rapports de l'IA, y compris les pistes d'audit et les références sources utilisées pour suivre et examiner les décisions de l'IA et leurs résultats.
Protocoles de traçabilité dans le développement de l'IA	Intégrer des protocoles de traçabilité dans les phases de développement et de déploiement de l'IA.
Revue régulières des processus décisionnels de l'IA	Programmer des revues régulières pour assurer la traçabilité continue des décisions de l'IA.
Rapports aux parties prenantes sur les décisions de l'IA	Établir des mécanismes de rapport pour communiquer la prise de décision de l'IA aux parties prenantes.

Considérations sur les contrôles des risques associés à l'évolution continue de la technologie

RISQUES

Cette catégorie de risque aborde la nécessité pour les organisations d'adapter la gouvernance de l'IA générative au rythme rapide des avancées technologiques de l'IA.

CONSIDÉRATIONS DE CONTRÔLE

Programme de surveillance de l'évolution technologique	Établir un programme dédié qui surveille en continu l'évolution de la technologie de l'IA générative. Le programme doit inclure des contributions d'un ensemble diversifié d'employés de l'organisation.
Revoir et mettre à jour le cadre de gouvernance	Revoir et mettre à jour régulièrement un cadre de gouvernance et des politiques pour refléter les changements significatifs des risques en raison des développements des capacités de l'IA.
Laboratoires d'innovation et programmes pilotes	Créer des laboratoires d'innovation ou des programmes pilotes pour expérimenter de nouvelles technologies d'IA dans un environnement contrôlé. Ces laboratoires peuvent fournir des informations sur les implications pratiques des technologies émergentes de l'IA et informer les stratégies de gestion des risques.

Transparence, responsabilité et amélioration continue

Considérations sur les contrôles des risques divers ou des risques conceptuels ou hypothétiques élevés

RISQUES

Cette catégorie de risque englobe une variété de risques tels que le manque de sensibilisation aux capacités et aux limitations de l'IA, le potentiel d'abus, les défis de la standardisation et les impacts géopolitiques ou géostratégiques sur les équilibres mondiaux dus à l'IA.

Cette catégorie de risque considère les risques théoriques que l'IA devienne incontrôlable ou atteigne un niveau de « superintelligence ».

CONSIDÉRATIONS DE CONTRÔLE

Programmes de sensibilisation et d'éducation sur l'IA	Développer et dispenser des programmes aux parties prenantes internes et/ou externes pertinentes pour améliorer la sensibilisation aux capacités, aux risques, aux limitations et à l'utilisation appropriée de l'IA.
Mécanismes de prévention des abus	Mettre en œuvre des mécanismes pour prévenir et détecter les utilisations abusives ou détournées des technologies de l'IA.
Équipes de réponse rapide et d'atténuation	Mettre en place des équipes de réponse rapide équipées pour gérer les incidents ou crises imprévus liés à l'IA. Ces équipes doivent avoir des protocoles clairs pour évaluer les situations, prendre des décisions et mettre en œuvre des stratégies d'atténuation rapidement pour minimiser l'impact.
Engagement et dialogue avec les parties prenantes	Faciliter un dialogue continu avec les parties prenantes, y compris les clients, les régulateurs et le public, pour discuter des préoccupations et des attentes liées à l'IA. Cet engagement peut aider à identifier les risques émergents et les préoccupations sociétales qui peuvent ne pas être immédiatement apparents.

À propos de nos auteurs



Scott A. Emett, PhD

Associate Professor, Arizona State University

Scott Emett est professeur associé à l'Université d'État de l'Arizona. Ses recherches examinent comment les producteurs et les consommateurs de divulgations financières prennent des jugements et des décisions, en se concentrant souvent sur la manière dont les perturbations technologiques influencent ces jugements et décisions. Il s'efforce de mener des recherches offrant des perspectives précieuses pour les praticiens du domaine, comblant ainsi le fossé entre la recherche académique et l'application pratique. Ses travaux ont été publiés dans des revues majeures telles que le *Journal of Accounting and Economics*, *The Accounting Review*, *Contemporary Accounting Research*, *Accounting, Organizations, and Society*, *Review of Accounting Studies* et *Auditing: A Journal of Practice and Theory*, entre autres.



Marc Eulerich, PhD, CIA

Dean and Professor, University of Duisburg-Essen

Marc Eulerich est titulaire de la chaire d'audit interne et doyen de la Mercator School of Management à l'Université de Duisburg-Essen, en Allemagne. Il dirige également le Center for Internal Auditing Excellence et le Mercator Audit & Artificial Intelligence Research Center (MAARC), tous deux situés dans la même université. Il a publié plus de 150 articles scientifiques et de praticiens ainsi que des livres sur la gouvernance d'entreprise, l'audit interne et la stratégie. Ses recherches sont publiées dans de nombreuses revues nationales et internationales. Le professeur Dr. Eulerich soutient également la profession mondiale de l'audit interne par de nombreuses conférences et projets de conseil afin d'intensifier la relation entre la théorie et la pratique.



Jason Pikoos

Managing Partner, Connor Group

Jason Pikoos est associé directeur et dirige les initiatives en matière de technologie et d'innovation chez Connor Group, y compris les solutions pilotées par l'IA générative (GenAI). Jason apporte plus de 20 ans d'expérience en comptabilité, opérations et technologie, travaillant avec des entreprises en forte croissance et technologiques. Il est un leader dans l'aide aux entreprises pour atteindre l'excellence opérationnelle grâce à l'amélioration des processus, à la technologie et à l'automatisation, aux données et à l'analytique, ainsi qu'à une gouvernance efficace. Jason est diplômé de l'Université de Cape Town et a passé plus de 10 ans dans la comptabilité publique avant de rejoindre Connor Group.



David A. Wood, PhD

Professor, Brigham Young University

David A. Wood est le professeur Glenn D. Ardis de comptabilité à l'Université Brigham Young. Avec plus de 160 publications dans des revues académiques et de praticiens respectées, des monographies, des livres et des études de cas, les recherches de David se concentrent sur la technologie, la gouvernance, la gestion des risques et les contrôles internes. Son travail influent lui a valu d'être reconnu comme l'une des 100 personnes les plus influentes dans le domaine de la comptabilité par *Accounting Today*. David collabore avec des entreprises de toutes tailles, des cabinets comptables et des régulateurs, fournissant des informations et une expertise sur les questions émergentes de gouvernance et de comptabilité.

À propos de nos soutiens



Connor Group (Sponsor and Contributor)

Connor Group est une société de services professionnels spécialisée, composée d'anciens de Big 4 et de cadres de l'industrie. Notre équipe de professionnels très expérimentés aide les dirigeants financiers et opérationnels à résoudre leurs questions les plus complexes et les plus importantes, y compris les solutions numériques, la comptabilité financière et les opérations, les services d'introduction en bourse (IPO) et de fusions et acquisitions (M&A), ainsi que les services gérés. Nos clients sont les entreprises les plus en croissance au monde, et nous les soutenons alors qu'ils changent le monde et créent de nouveaux marchés !

connorgp.com

[AI & Automation Landing Page](#)



Boomi (Reviewer and Contributor)

Boomi propulse l'avenir des affaires grâce à l'intégration et à l'automatisation intelligentes. En tant qu'entreprise de logiciels en tant que service (SaaS) leader dans sa catégorie au niveau mondial, Boomi célèbre plus de 20 000 clients dans le monde entier et un réseau mondial de 800 partenaires. Les organisations se tournent vers la plateforme primée de Boomi pour connecter leurs applications, leurs données et leurs collaborateurs afin d'accélérer leur transformation numérique. Pour plus d'informations, visitez boomi.com.

boomi.com

[AI & Automation Landing Page](#)

We thank Mélissa Fortin ([linkedin.com/in/mélissa-fortin-31843473/](https://www.linkedin.com/in/mélissa-fortin-31843473/)) for her assistance with the translation.