Liste de vérification — Préparation à la conformité IA

Outil pratique pour évaluer vos pratiques actuelles et repérer les écarts en gouvernance et gestion des risques

Septembre 2025

AVERTISSEMENT (traduction) : Cette liste est fournie à titre de recommandation générale et ne constitue pas un avis juridique. Adaptez-la avec votre CISO, vos conseillers juridiques ou votre équipe conformité avant toute mise en œuvre.

Table des matières

1) Direction et imputabilité

Identifiez clairement qui porte les risques IA et comment l'information circule vers la haute direction.

☐ Désigner un responsable exécutif (p. ex. chef de l'exploitation, conseiller juridique, CISO) avec budget.

☐ Intégrer l'IA aux tableaux de bord trimestriels du CA/comité des risques.

☐ Approuver un ensemble de contrôles IA (Utilisation acceptable, Risque des modèles, Fournisseurs, Rétention, Invite sécurisée).

☐ Tenir un registre IA couvrant les outils internes, le SaaS et les fonctions intégrées (signature, e-découverte, portail client).

☐ Arrimer les risques IA à la taxonomie d'entreprise avec seuils et déclencheurs.

Notes / decisions: _____

2) Registre des cas d'usage et triage

Tous les cas d'usage ne se valent pas : recensement, classement, puis contrôle.

☐ Recenser les usages par groupe de pratique (litige, fiscalité, audit, KM/connaissances).

☐ Repérer les données personnelles et les informations privilégiées; marquer les ensembles réglementés.

☐ Coter le risque intrinsèque (vie privée, équité, sécurité, finances, réputation) et définir des paliers de contrôle.

☐ Effectuer une EFVP/PIA en présence de données personnelles/inférées; documenter les mesures d'atténuation.

Notes / decisions: _____

3) Données et vie privée (Loi 25, CPPA/LPRPDE)

La qualité des données et la transparence priment avant l'invite.

☐ Mettre à jour les avis de transparence et la base légale lorsque des données personnelles sont traitées.

☐ Appliquer la minimisation; fixer la rétention pour journaux, sorties et ensembles d'entraînement/évaluation.

☐ Dé-identification/pseudonymisation et chiffrement en transit/au repos pour les données sensibles.

☐ Évaluer les transferts transfrontaliers; clauses contractuelles et, au besoin, localisation.

☐ Opérationnaliser les droits des personnes : accès, correction, explication pour les décisions assistées par IA.

Notes / decisions: _____

4) Cycle de vie des modèles et systèmes

Les modèles évoluent; votre contrôle doit suivre le rythme.

☐ Tracer la provenance et les versions; tenir une nomenclature simple (MBOM).

☐ Essais pré-déploiement : biais/exactitude/toxicité/robustesse et red teaming ciblé.

☐ Humain dans la boucle pour les automatisations à fort impact client.

☐ Rassembler la justification et les résumés d'explicabilité lorsque des droits sont en jeu.

☐ Gérer les changements avec critères de retour arrière, approbations et notes de version.

Notes / decisions: _____

5) Sécurité et résilience

Prévoyez des invites curieuses… et des attaquants créatifs.

☐ Atténuer l'injection d'invite, l'exfiltration et les abus de récupération; assainir entrées/sorties.

☐ Isoler secrets et clés API; limites de débit et détection d'anomalies.

☐ Journaliser les interactions et la dérive; alerter sur contournements et sorties anormales.

☐ Tester la sauvegarde/PRA pour jeux de données, magasins vectoriels et artefacts de modèle.

☐ Planifier des tests de sécurité indépendants et des exercices de red teaming IA.

Notes / decisions: _____

6) Risques fournisseurs (tiers)

Votre exposition inclut les plateformes et modèles externes.

☐ Contractualiser les frontières de données (pas d'entraînement, protection de la PI, suppression à la sortie).

☐ Examiner SOC 2/ISO 27001 et les engagements de confidentialité; historiser les incidents.

☐ Réaliser des évaluations de risque des modèles tiers et les actualiser sur une cadence définie.

☐ Prévoir le désengagement : restitution/suppression des données, portabilité et continuité.

Notes / decisions: _____

7) IA responsable et éthique

Des principes concrets, mesurables et testés.

☐ Adopter des principes mesurables (équité, responsabilité, transparence) et définir les tests associés.

☐ Élaborer des plans d'atténuation des biais; tester les effets sur catégories protégées.

☐ Publier un canal de signalement (courriel éthique) et suivre les délais de traitement.

☐ Prendre en compte l'accessibilité et l'inclusion dans les services activés par l'IA.

Notes / decisions: _____

8) Exploitation et surveillance

Piloter ce que l'on voit.

☐ Définir des KPIs/KRIs (taux de faux positifs, dérive, incidents de sécurité, latence/coûts).

☐ Planifier les tests de contrôle; centraliser les preuves avec responsables désignés.

☐ Utiliser les résultats pour améliorer invites, garde-fous et données d'entraînement.

Notes / decisions: _____

9) Incidents et escalades

La rapidité et la clarté font la différence.

☐ Préparer des playbooks (hallucination, fuite, compromission, contenu nuisible).

☐ Cartographier seuils et délais réglementaires (Loi 25, CPPA/LPRPDE) et les responsabilités d'avis.

☐ Pré-approuver les communications clients/régulateurs; exercices semestriels.

☐ Capitaliser les leçons apprises et suivre les actions correctives/préventives (CAPA).

Notes / decisions: _____

10) Personnes et formation

L'adoption est d'abord humaine.

☐ Former par rôle (avocats, CPA, développeurs, soutien).

☐ Diffuser les lignes directrices d'invite sécurisée et d'utilisation acceptable; exiger l'attestation.

☐ Intégrer deepfakes et harponnage social à la sensibilisation.

Notes / decisions: _____

11) Preuves et auditabilité

Sans preuve, pas de contrôle.

☐ Maintenir un registre central (politiques, essais, approbations, EFVP/PIA).

☐ Assurer la traçabilité risques → contrôles → tests → enjeux → actions.

☐ Structurer les artefacts par familles de contrôles pour accélérer les revues.

Notes / decisions: _____

12) Feuille de route et budget

Prioriser et démontrer l'avancement.

☐ Cartographier les écarts; gains rapides (30–60 j), moyen terme (90–180 j), long terme (180+ j).

☐ Attribuer responsables, budgets et jalons; publier un tableau de bord simple.

Notes / decisions: _____

Niveaux de maturité (auto-évaluation)

Level	What this looks like
0 — Non démarré	Aucune responsabilité claire; pas de contrôle ni de preuve.
1 — Rédaction	Politiques/contrôles rédigés; pilotes en cours.
2 — Implanté	Contrôles en place; fonctionnement documenté régulièrement.
3 — Mesuré	Indicateurs suivis; essais périodiques et optimisations.
4 — Optimisé	Amélioration continue pilotée par les métriques et les risques.

Feuille de pointage

Domaine	Éléments complétés	Total	Score (0–4)	Responsable	Échéance
1) Direction et imputabilité					
2) Registre des cas d'usage et triage					
3) Données et vie privée (Loi 25, CPPA/LPRPDE)					
4) Cycle de vie des modèles et systèmes					
5) Sécurité et résilience					
6) Risques fournisseurs (tiers)					
7) IA responsable et éthique					
8) Exploitation et surveillance					
9) Incidents et escalades					
10) Personnes et formation					
11) Preuves et auditabilité					
12) Feuille de route et budget					