La réglementation en un coup d'œil : règlement européen sur l'IA, ISO/IEC 42001 et NIST AI RMF

Un instrument gratuit de AI GOVERNANCE CHAIN™. La carte est gratuite. Les packs de conformité qui satisfont chaque exigence constituent le parcours payant.

Abréviations et acronymes

Cette section définit chaque acronyme utilisé dans ce document. Aucune connaissance préalable n'est supposée.

- IA : intelligence artificielle.
- UE : Union européenne.
- Règlement européen sur l'IA : le règlement (UE) 2024/1689 du Parlement européen et du Conseil, la première loi complète au monde sur l'intelligence artificielle.
- ISO/IEC 42001 : la norme internationale de système de management de l'intelligence artificielle, publiée en décembre 2023 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC).
- NIST AI RMF : le cadre de gestion des risques de l'IA (AI Risk Management Framework) publié par le National Institute of Standards and Technology des États-Unis.

À qui s'adresse cette carte

Aux responsables de la conformité, aux dirigeants et aux architectes qui ont besoin de comprendre, sur une seule page, les trois références qui structurent désormais la gouvernance de l'IA dans le monde, et la manière dont elles s'articulent.

Pourquoi cette carte existe (le POURQUOI)

Trois instruments distincts dominent la conversation sur la gouvernance de l'IA. Ils sont souvent confondus, alors qu'ils font des travaux différents : l'un est une loi, l'autre est une norme certifiable, le troisième est un cadre volontaire. Savoir lequel est lequel, et ce que chacun exige, fait la différence entre un effort ciblé et un effort gaspillé.

Les trois instruments en un coup d'œil

1. Le règlement européen sur l'IA (la loi)

- Ce que c'est. Le règlement de l'Union européenne sur l'intelligence artificielle, la première loi complète de ce type. Il est contraignant.

- Comment il fonctionne. Il classe les systèmes d'IA par niveaux de risque : risque inacceptable (pratiques interdites), haut risque (obligations strictes), risque limité (devoirs de transparence) et risque minimal (largement libre).
- Pourquoi il compte. Il s'applique aux organisations qui mettent des systèmes d'IA sur le marché de l'UE ou dont les sorties d'IA sont utilisées dans l'UE, quel que soit le lieu d'établissement de l'organisation. Ses obligations entrent en vigueur de manière échelonnée, selon un calendrier publié.
- Qui doit s'en soucier en priorité. Toute organisation exploitant une IA à haut risque ayant un lien avec l'UE.

2. ISO/IEC 42001 (la norme certifiable)

- Ce que c'est. La première norme internationale de système de management pour l'intelligence artificielle, publiée en décembre 2023.
- Comment elle fonctionne. Elle définit les exigences d'un système de management de l'IA : politiques, objectifs, contrôles, rôles et amélioration continue. Une organisation peut être certifiée de manière indépendante sur cette base.
- Pourquoi elle compte. La certification apporte une preuve externe et vérifiable qu'une organisation gouverne l'IA de manière systématique. Elle est de plus en plus demandée dans les achats et les partenariats.
- Qui doit s'en soucier en priorité. Les organisations qui veulent démontrer leur maturité de gouvernance à leurs clients, à leurs régulateurs ou à leurs partenaires.

3. Le NIST AI RMF (le cadre volontaire)

- Ce que c'est. Le cadre de gestion des risques de l'IA du National Institute of Standards and Technology des États-Unis. C'est une orientation volontaire, pas une loi.
- Comment il fonctionne. Il est organisé autour de quatre fonctions : gouverner (fixer la culture et la supervision), cartographier (comprendre le contexte et le risque), mesurer (évaluer et suivre le risque) et gérer (agir sur le risque).
- Pourquoi il compte. C'est une structure pratique et largement adoptée pour bâtir un programme d'IA fondé sur le risque, et elle se projette proprement sur le règlement européen sur l'IA comme sur ISO/IEC 42001.
- Qui doit s'en soucier en priorité. Toute organisation qui construit un programme de risque, en particulier celles qui veulent une structure faisant le pont entre la loi et la certification.

Comment les trois s'articulent

La loi vous dit ce que vous devez faire. La norme vous permet de prouver que vous le faites. Le cadre vous donne une méthode pour y parvenir. Une organisation sérieuse utilise les trois : le règlement européen sur l'IA fixe les obligations, le NIST AI RMF structure le travail, ISO/IEC 42001 en apporte la preuve certifiable.

Où s'arrête la couche gratuite et où commence le parcours payant

Cette carte vous donne le QUOI et le POURQUOI : les trois références et leur logique. La couche payante vous donne le COMMENT : le Pack de conformité au règlement européen sur l'IA, la Boîte à outils de certification ISO/IEC 42001 et le Cahier d'exercices NIST AI RMF, chacun avec les documents de travail qui satisfont les exigences.

- Pour le COMMENT : les packs de conformité.
- Pour l'AVEC-VOUS : The Governance Circle.
- Pour le FAIT-POUR-VOUS : l'Audit de gouvernance pré-déploiement.

AI GOVERNANCE CHAIN™
Cadre de gouvernance de l'IA

Membre du conseil consultatif de la Harvard Business Review.
Norme documentaire de AI GOVERNANCE CHAIN™ : une gouvernance de l'IA centrée sur l'humain.