

NOTE DE SYNTHÈSE — GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE

ISO/IEC 42001

Système de Management de l'Intelligence Artificielle (SMIA)

Comprendre le premier référentiel international certifiable de gouvernance de l'IA, sa structure, son coût de mise en œuvre et son articulation avec les cadres réglementaires en vigueur.

Mohammed El Bouzidi

Consultant Senior & Ingénieur de Formation — Développement Organisationnel · Stratégie & Développement RH · Gouvernance Territoriale · Gouvernance IA

NAITECH Consult — Maroc · Afrique | Juillet 2026

EN BREF

- Publiée le 18 décembre 2023 par l'ISO/IEC (comité technique SC 42), c'est la première norme internationale certifiable dédiée au management de l'intelligence artificielle.
- Sa structure reprend le socle commun des systèmes de management ISO — 10 clauses et une annexe de mesures — déjà familière aux organisations certifiées ISO 9001 ou ISO 27001.
- Elle couvre une part significative, mais pas la totalité, des exigences du règlement européen sur l'IA (AI Act) — sans en constituer une preuve de conformité automatique.
- Aucune obligation réglementaire ne l'impose aujourd'hui au Maroc ou en Afrique : c'est donc une fenêtre de positionnement, plus qu'une contrainte.

01 Qu'est-ce que la norme ISO/IEC 42001 ?

Un système de management de l'IA (SMIA) est un ensemble structuré de politiques, de processus et de mesures de contrôle permettant à une organisation de piloter la conception, le déploiement et l'exploitation de ses systèmes d'intelligence artificielle. ISO/IEC 42001 en fixe les exigences : elle s'adresse à toute organisation, quelle que soit sa taille ou son secteur, qui conçoit, fournit ou utilise des systèmes d'IA.

La norme est volontaire — aucune loi n'impose aujourd'hui de s'y conformer — mais elle est conçue pour être auditable, exactement comme ISO 9001 pour la qualité ou ISO 27001 pour la sécurité de l'information. Une organisation peut donc choisir de l'appliquer en interne comme cadre de bonnes pratiques, ou d'aller jusqu'à la certification par un organisme accrédité, pour en faire une preuve tangible vis-à-vis de ses clients, partenaires ou régulateurs.

02 Le contexte 2026 : pourquoi maintenant

Trois dynamiques convergent depuis 2024 et expliquent l'intérêt croissant porté à cette norme.

Un signal de marché fort

Amazon Web Services a fait certifier plusieurs de ses services d'IA (Bedrock, Q Business, Textract, Transcribe) dès novembre 2024. Anthropic a obtenu sa certification en janvier 2025, suivie par Microsoft pour Azure AI Foundry et Security Copilot en juillet 2025. La certification s'installe progressivement comme un prérequis implicite dans les cycles d'achat d'entreprise.

Une pression réglementaire croissante

Le règlement européen sur l'IA (AI Act) est entré en vigueur en 2024, avec une application progressive : interdictions de certaines pratiques dès février 2025, obligations pour les modèles à usage général dès août 2025, puis un régime spécifique pour les systèmes à haut risque. Un accord politique conclu en mai 2026 (« Omnibus IA ») a repoussé une partie de ce dernier calendrier à décembre 2027, voire août 2028 pour l'IA intégrée dans certains produits — un signe que le cadre reste mouvant, mais que la trajectoire est claire.

Un écosystème de normes qui se structure

L'ISO a complété 42001 par des textes connexes : ISO/IEC 23894 (gestion des risques liés à l'IA), ISO/IEC 42005 (évaluation d'impact d'un système IA) et, plus récemment, ISO/IEC 42006 (2025), qui encadre les organismes habilités à délivrer la certification elle-même.

03 Architecture du référentiel : les clauses 4 à 10

ISO/IEC 42001 reprend la structure-cadre commune à la plupart des normes de management ISO — la même qu'ISO 9001 ou ISO 27001 — organisée autour du cycle Planifier-Déployer-Vérifier-Améliorer.

Clause	Contenu
Clause 4 — Contexte	Périmètre du SMIA, parties prenantes, enjeux internes et externes.
Clause 5 — Leadership	Engagement de la direction, politique IA, rôles et responsabilités.
Clause 6 — Planification	Identification et traitement des risques et opportunités liés à l'IA ; objectifs mesurables.
Clause 7 — Support	Ressources, compétences, sensibilisation, communication, documentation.
Clause 8 — Fonctionnement	Mise en œuvre opérationnelle des processus ; évaluation d'impact des systèmes IA.
Clause 9 — Évaluation des performances	Surveillance, audit interne, revue de direction.
Clause 10 — Amélioration	Traitement des non-conformités, amélioration continue.

04 Annexe A : 38 mesures réparties en 9 domaines

L'annexe A rassemble 38 mesures de référence, réparties en neuf domaines. Elles ne sont pas toutes obligatoires : chaque organisation sélectionne les mesures pertinentes au regard de son analyse de risque (clause 6.1.3) et consigne ses choix — inclusions et exclusions justifiées — dans une Déclaration d'applicabilité (SoA).

Domaine (Annexe A)	Ce qu'il couvre concrètement
A.2 — Politiques liées à l'IA	Formalisation d'une politique IA, alignée sur les autres politiques internes, revue à intervalles réguliers.
A.3 — Organisation interne	Rôles et responsabilités attribués ; procédure de signalement des préoccupations liées à l'IA.
A.4 — Ressources	Documentation des composants et actifs des systèmes IA ; gestion de la provenance et de la qualité des ressources mobilisées.
A.5 — Évaluation d'impact	Analyse des impacts potentiels — biais, discrimination, atteintes physiques, psychologiques ou financières — avant tout déploiement, avec un niveau de contrôle proportionné au risque identifié.
A.6 — Cycle de vie des systèmes IA	Gouvernance de la conception au retrait : développement, validation, déploiement, surveillance des dérives, décommissionnement.
A.7 — Données	Qualité, provenance, traçabilité et protection des données utilisées pour entraîner ou faire fonctionner les systèmes.
A.8 — Information des parties prenantes	Transparence sur le fonctionnement, les limites et les décisions produites par les systèmes IA.
A.9 — Utilisation des systèmes IA	Contrôle humain effectif : déclencheurs d'intervention, capacité de correction ou d'arrêt.
A.10 — Relations avec les tiers	Évaluation des fournisseurs d'IA, clauses contractuelles adaptées, surveillance continue des systèmes fournis par des tiers.

05 Les annexes B, C et D

- Annexe B (informative) — un guide de mise en œuvre détaillant, mesure par mesure, ce qu'une organisation peut concrètement mettre en place.
- Annexe C — un référentiel d'objectifs types et de sources de risque propres à l'IA (biais, dérive de modèle, perte d'explicabilité...), utile pour cadrer une analyse de risque ou aligner les parties prenantes.
- Annexe D — un guide d'articulation avec d'autres systèmes de management (ISO/IEC 27001, ISO/IEC 27701, ISO 9001, normes sectorielles), pour éviter de reconstruire une gouvernance à partir de zéro lorsqu'un système existe déjà.

06 Processus et budget de certification

La certification suit le schéma classique des systèmes de management ISO, conduit par un organisme certificateur accrédité (BSI, DNV, SGS, Bureau Veritas, TÜV Rheinland, entre autres).

Étape	Durée indicative	Contenu
Analyse d'écart	2 semaines à 3 mois	Comparaison de l'existant avec les exigences de la norme, priorisation des écarts.

Étape	Durée indicative	Contenu
Conception du SMIA	1 à 3 mois	Politique IA, cartographie des risques, gouvernance des données, Déclaration d'applicabilité.
Mise en œuvre & sensibilisation	1 à 4 mois	Formation des équipes, fonctionnement réel sous le nouveau système.
Audit interne	≈ 1 mois	Revue indépendante en amont de l'audit externe.
Audit — Étape 1	1 à 2 jours	Revue documentaire : politiques, analyse de risque, Déclaration d'applicabilité.
Audit — Étape 2	4 jours et plus	Vérification de la mise en œuvre réelle sur le terrain.

Au total, la démarche s'étale généralement sur 3 à 12 mois — 4 à 6 mois pour une organisation déjà certifiée ISO 27001, qui réutilise une bonne partie de sa gouvernance existante. Le coût dépend fortement du périmètre retenu : il va de quelques milliers de dollars pour une structure de petite taille certifiant un périmètre restreint, à plusieurs dizaines de milliers de dollars pour un périmètre étendu ou une organisation de taille importante. Le certificat, une fois obtenu, reste valable trois ans, sous réserve d'audits de surveillance annuels.

07 Articulation avec les autres référentiels

Référentiel	Nature	Lien avec ISO 42001
Règlement européen sur l'IA (AI Act)	Obligation légale (UE)	Couvre une part substantielle des exigences des articles 9 à 17 — gestion des risques, gouvernance des données, documentation technique, transparence, contrôle humain — sans dispenser d'une analyse spécifique au règlement.
ISO/IEC 23894	Guide non certifiable	Approfondit la méthodologie de gestion des risques liés à l'IA, en appui de la clause 6.1 d'ISO 42001.
ISO/IEC 42005	Guide non certifiable	Propose une méthodologie d'évaluation d'impact d'un système IA donné sur les personnes, la société et l'environnement.
ISO/IEC 42006 (2025)	Norme technique	Fixe les exigences applicables aux organismes habilités à auditer et certifier les SMIA.
NIST AI RMF	Cadre volontaire (États-Unis), non certifiable	Structuré en quatre fonctions — Gouverner, Cartographier, Mesurer, Gérer — souvent utilisé en amont d'ISO 42001 comme méthodologie de gestion des risques.

08 Une opportunité pour les structures agiles marocaines et africaines

Aucune obligation réglementaire locale n'impose aujourd'hui ISO/IEC 42001 aux organisations marocaines ou africaines. C'est précisément ce qui en fait une opportunité plutôt qu'une contrainte : contrairement à une grande organisation qui doit faire cohabiter cette démarche avec des systèmes existants complexes, une PME ou une structure de taille moyenne peut circonscrire un périmètre restreint — un produit, un service ou un usage précis de l'IA — et avancer avec l'agilité qui la caractérise déjà.

La sélection des mesures via la Déclaration d'applicabilité rend la démarche proportionnée : il ne s'agit pas d'appliquer les 38 mesures indistinctement, mais de construire une gouvernance calibrée au risque réel de l'organisation. Pour un cabinet de conseil en gouvernance et développement organisationnel, cela ouvre une offre naturelle : diagnostic de maturité IA, cartographie des risques, accompagnement à la Déclaration d'applicabilité, préparation à un audit à blanc — autant de missions qui prolongent des compétences déjà mobilisées en gouvernance territoriale et en stratégie RH, avant que la certification ne devienne un standard de facto exigé par les grands donneurs d'ordre internationaux.

09 Ressources documentaires de référence

- ISO — page officielle de la norme : [iso.org/standard/42001](https://www.iso.org/standard/42001) (texte intégral disponible à l'achat, publication sous licence).
- ISO — « ISO 42001 explained », présentation introductive publiée par l'organisation elle-même.
- NIST — passerelle officielle entre l'AI RMF et ISO/IEC 42001 (crosswalk), disponible sur airc.nist.gov.
- Normes complémentaires disponibles sur [iso.org](https://www.iso.org) : ISO/IEC 23894, ISO/IEC 42005, ISO/IEC 42006.

Document préparé par NAITECH Consult à titre de synthèse professionnelle. Il ne constitue pas un avis juridique et ne remplace pas la lecture du texte intégral de la norme.