FeelAgile

Guide

ISO 42001

Système de Management de l'Intelligence Artificielle

Intelligence artificielle, le grand bouleversement

Maîtriser l'IA

En quelques années, l'intelligence artificielle est devenue omniprésente dans nos environnements professionnels.
Ce qui relevait hier du laboratoire s'est infiltré dans toutes les couches de l'entreprise, parfois sans que l'on s'en rende compte.

Aujourd'hui, les grands modèles de langage (LLM), comme ChatGPT, Claude ou Gemini, sont utilisés au quotidien pour rédiger, résumer, traduire, coder ou analyser.
Ils sont intégrés dans les outils bureautiques, les plateformes collaboratives, les environnements de développement et même les systèmes de cybersécurité. Ces usages internes se multiplient, souvent sans cadre clair, posant des questions de confidentialité, de fiabilité et de responsabilité.

Parallèlement, une autre vague se déploie : celle du développement d'applications et de produits à base d'IA. Les entreprises intègrent désormais des composants intelligents dans leurs logiciels, leurs services clients, leurs plateformes SaaS ou leurs outils d'analyse.
Cela transforme profondément les chaînes technologiques : infrastructures cloud, flux de données, gouvernance des modèles, sécurité applicative... tout l'écosystème doit s'adapter.
Cette prolifération rapide crée un paradoxe : jamais l'IA n'a offert autant de puissance, et jamais les organisations ne se sont senties aussi démunies face à sa maîtrise.
Entre innovation accélérée et zones d'ombre réglementaires, de nombreuses entreprises ont le sentiment de perdre le contrôle sur des usages qu'elles n'ont pas toujours anticipés.

L'IA n'est plus un outil ponctuel : elle structure désormais les processus, influence les décisions, et devient un composant critique des systèmes d'information.

Bref, l'IA est partout, et cette omniprésence impose une nouvelle discipline : la maîtrise de l'IA.

Sommaire

ISO 42001, mon parcours vers une IA de confiance

CONTEXTE

Pourquoi une norme sur L'IA ?

01

Les nouveaux risques

On ne pilote pas l'IA avec un interrupteur, mais avec un système de management

L'usage massif de l'intelligence artificielle fait apparaître de nouveaux risques, souvent sous-estimés.

Dans les entreprises, le "Shadow AI" devient un vrai sujet : des salariés utilisent des outils d'IA générative sans cadre ni validation.
Résultat : des données sensibles sont partagées sur des plateformes publiques, du code est produit sans contrôle. À dire vrais, je pense que le Shadow AI est aussi dangereux que l'absence d'IA. **Manquer l'opportunité de l'IA est certainement le plus gros risque.**

Cela crée donc des multiples risques : fuite d'informations, non-conformité RGPD et perte de maîtrise.

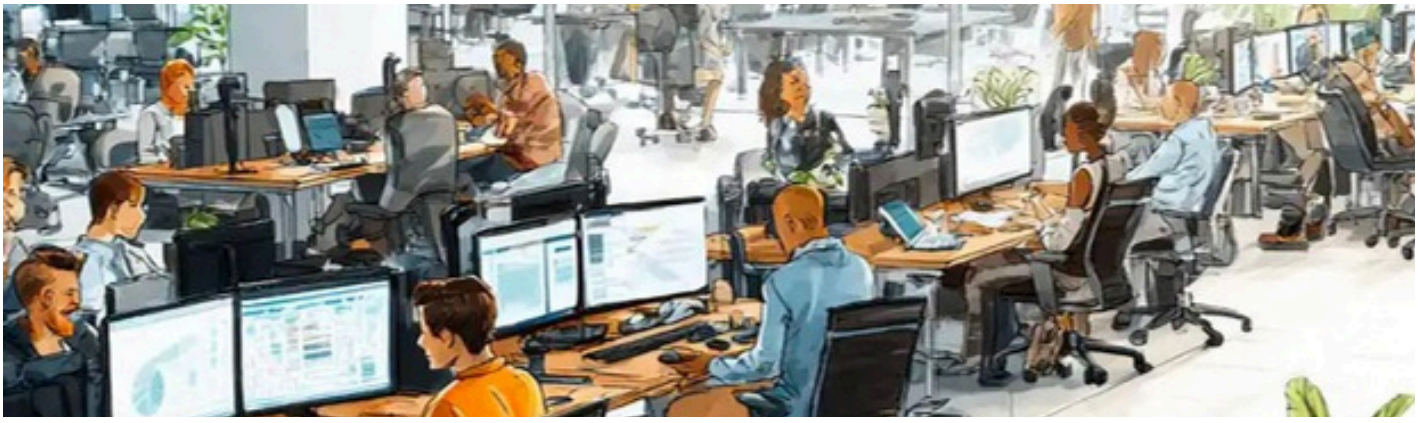
Des entreprises d'IA

Pour les entreprises qui développent des solutions intégrant de l'IA, les enjeux sont encore plus importants. Il faut gérer la sécurité des modèles, la conformité aux réglementations (AI Act, RGPD, NIS2), et garantir la transparence des algorithmes. Une faille ou un biais dans un modèle peuvent impacter directement les utilisateurs ou engager la responsabilité de l'entreprise.

Des risques systémiques

Ces risques ne sont pas seulement locaux : ils deviennent systémiques. L'IA alimente des processus critiques (finance, santé, cybersécurité) et une erreur peut se propager très vite. La décision d'OpenAI d'ajouter un bouton d'arrêt physique à ses systèmes illustre bien cette inquiétude : même les leaders du domaine craignent la perte de contrôle.

C'est là qu'intervient l'ISO 42001. Plutôt que de réagir dans l'urgence, elle propose une méthode claire pour gouverner les usages de l'IA, identifier les risques, définir les responsabilités et assurer une maîtrise continue. En somme, passer de la peur du dérapage à la confiance maîtrisée.



Les besoins : transparence, gouvernance, confiance, maîtrise et performance

Le premier besoin face à l'essor de l'IA n'est pas seulement de contrôler, mais de transformer. L'intelligence artificielle bouleverse les modes de décision, les flux de données et les chaînes de valeur : elle impose une nouvelle manière de penser la gouvernance des technologies.

Et pour être franc, personne ne sait vraiment où cela va. Même dans le domaine du logiciel, il devient difficile de prévoir comment vont évoluer les produits, les architectures et les méthodes de développement.

Mais le risque n°1, aujourd'hui, c'est l'inaction. Face à une technologie qui avance aussi vite, ne rien faire, attendre ou observer, revient à se faire dépasser. Il faut au contraire agir, être performant, et clarifier ses intentions : que veut-on faire de l'IA ? Souhaite-t-on devenir développeur de solutions IA, intégrateur de modèles dans ses produits, ou simplement utilisateur éclairé ?

Répondre à cette question, c'est déjà reprendre le contrôle et donner un sens à sa stratégie.

Les entreprises doivent ensuite instaurer de la transparence : comprendre comment les modèles fonctionnent, quelles données ils utilisent, et quelles limites ils comportent. Cette visibilité est indispensable pour instaurer la confiance, aussi bien en interne qu'auprès des clients, partenaires et régulateurs.

Vient ensuite la gouvernance : définir qui décide, qui surveille, et comment les risques sont traités. Sans cadre, les usages de l'IA se dispersent et perdent toute cohérence. La maîtrise devient donc essentielle — il s'agit de garder la main sur les outils, les modèles et les décisions qu'ils influencent.

Enfin, au-delà de la conformité et de la sécurité, un besoin émerge souvent oublié : la performance. L'IA doit être au service de la valeur, pas une source de complexité supplémentaire.

C'est tout l'enjeu de l'ISO 42001 : permettre aux organisations de transformer leur usage de l'IA en un levier de confiance et de performance durable.

Je veux me certifier ISO 42001, mais je veux que cela m'aide concrètement à développer l'IA

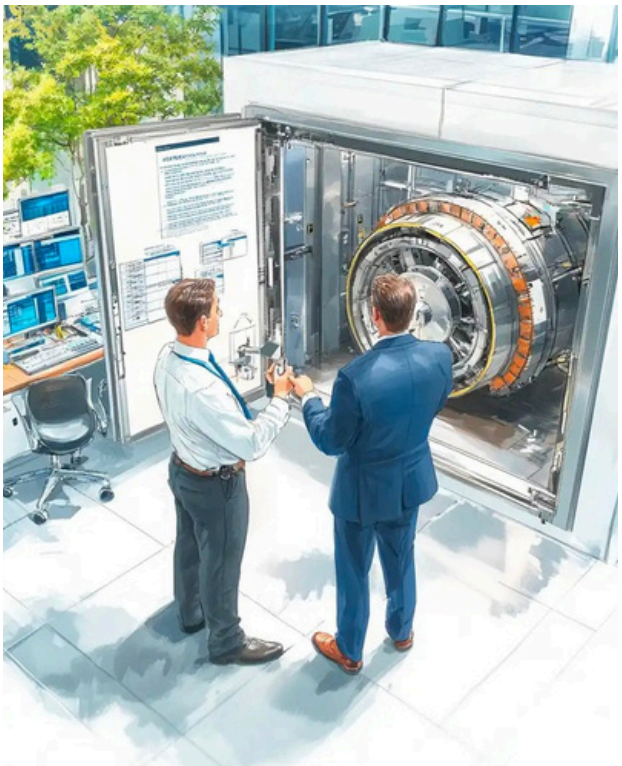
ISO 42001
Game Changer en confiance numerique

ISO 42001 est la première norme internationale de système de management dédiée à l'intelligence artificielle (AI Management System)

Entreprises emblématiques certifiées ISO/IEC 42001

Depuis sa publication fin 2023, la norme ISO/IEC 42001 attire l'attention des grands acteurs mondiaux de la tech, désireux de démontrer une gouvernance responsable et maîtrisée de l'intelligence artificielle.
Plusieurs entreprises emblématiques ont déjà franchi le pas.

- **Amazon Web Services (AWS)** a été l'un des premiers fournisseurs cloud à obtenir une certification accréditée, marquant un tournant pour la gouvernance des modèles d'IA à grande échelle.
- **Cognizant**, géant du conseil technologique, a également obtenu la certification pour son système de management de l'IA, affirmant sa volonté d'intégrer la conformité et l'éthique dans ses offres IA.



Pourquoi rejoindre les géants de la TECH ?

Des acteurs majeurs comme Amazon Web Services, Cognizant, Mimecast, HERE Technologies, Infosys, Dataminr, JAGGAER, Whistic ou Synthesia comptent parmi les premiers certifiés ISO 42001, aux côtés de nombreuses autres entreprises engagées dans une IA plus transparente, responsable et maîtrisée.

Rejoindre les géants de la tech certifiés ISO 42001, c'est affirmer son engagement à développer une IA de confiance, éthique et sécurisée, selon les plus hauts standards internationaux.

ISO 42001

Des DSI aux éditeurs SaaS : la transformation IA est en marche

Une norme de management, pas un simple cadre technique

L'ISO 42001 ne dit pas comment concevoir une IA, mais comment créer une dynamique IA de confiance.

Elle s'inscrit dans la lignée des grandes normes de management comme l'ISO 9001 (qualité) ou l'ISO 27001 (sécurité).

L'objectif n'est pas la conformité pour la conformité, mais **la mise en place d'une vraie méthode de pilotage : planifier, encadrer et améliorer les usages de l'IA dans le temps.**

C'est une norme souple et pragmatique, pensée pour vous aider à mieux intégrer l'IA et à créer une dynamique IA durable dans l'entreprise.

Concilier confiance, maîtrise et performance

L'ISO 42001 ne cherche pas à freiner l'innovation : elle aide à la rendre sûre, maîtrisée et performante.

Elle place la confiance au centre — confiance dans les données, les modèles, les décisions — mais ajoute une exigence souvent oubliée : la performance opérationnelle.

Gouverner, ce n'est pas freiner : c'est garantir que l'IA reste utile, responsable et performante.

Entreprises tech : encadrer et valoriser l'innovation

Pour les acteurs technologiques — éditeurs SaaS, startups IA, plateformes cloud — la norme permet de structurer la gouvernance et de montrer la fiabilité des modèles.

Elle devient un argument commercial fort pour rassurer clients et partenaires, tout en alignant innovation et conformité (AI Act, RGPD...).

DSI : reprenez la main

Face à la prolifération des usages internes tels que les LLM, l'automatisation ou l'analyse prédictive, l'ISO 42001 offre aux DSI et responsables IA un cadre pour reprendre le contrôle.

Elle facilite la cartographie des usages, l'évaluation des risques, et l'encadrement des expérimentations, tout en préservant la créativité des équipes. C'est un levier concret pour transformer la Shadow IA en une gouvernance maîtrisée et responsable.

CEO, dirigeants : piloter la transformation

Pour les directions générales et les risk managers, cette norme offre un cadre pour anticiper les risques et piloter la transformation IA avec confiance.

Elle aligne les équipes innovation, sécurité et conformité autour d'un langage commun et d'une vision claire : faire de l'IA un levier stratégique, pas un risque incontrôlé.

Fiche pratique

ISO 42001 : pourquoi et pour qui ?

Pourquoi passer la certification ISO 42001 ?

Piloter la performance de l'IA

- Gérer les risques de l'IA en interne à votre entreprise
- Renforcer la confiance de vos clients et partenaires dans le développement de l'IA
- Valoriser vos offres vis-à-vis de la concurrence en intégrant l'IA de façon maîtrisée

Pour qui ?

- Les DSI de grands groupes
- Les ESN, Assur-Tech
- Les développeurs de modèles d'IA
- Les développeurs de systèmes d'IA
- Toute entreprise qui utilise l'IA

Les bénéfices de la démarche

- Clarifier comment vous voulez utiliser l'IA
- Mieux maîtriser l'environnement global de l'IA et de ses transformations !
- Valoriser votre entreprise
- Innover et contrôler

Les objectifs de maîtrise de l'IA

Dans la démarche, vous allez déterminer les objectifs liés à l'IA importants dans votre démarche, comment vous voulez maîtriser l'IA :

- Responsabilité (Accountability) : L'IA modifie les cadres de responsabilité, car les décisions peuvent désormais dépendre d'un système plutôt que d'une personne.
- Expertise en IA (AI expertise) : L'organisation doit disposer de spécialistes interdisciplinaires capables de concevoir, évaluer et déployer des systèmes d'IA fiables.
- Qualité des données (Availability and quality of data) : Les systèmes d'IA doivent s'appuyer sur des données d'entraînement, de validation et de test disponibles et de qualité suffisante.
- Impact environnemental (Environmental impact) : L'IA peut réduire ou accroître l'empreinte environnementale selon son usage et la consommation de ressources qu'elle implique.
- Équité (Fairness) : Un usage inapproprié de l'IA peut générer des biais ou des discriminations dans les décisions automatisées.
- Maintenabilité (Maintainability) : L'organisation doit pouvoir modifier le système d'IA pour corriger les erreurs ou l'adapter à de nouvelles exigences.
- Vie privée (Privacy) : Une mauvaise gestion des données personnelles ou sensibles peut nuire gravement aux personnes concernées.
- Robustesse (Robustness) : Le système d'IA doit maintenir ses performances dans des conditions réelles, au-delà des seules données d'entraînement.
- Sûreté (Safety) : Le système doit éviter tout risque pour la vie humaine, la santé, les biens ou l'environnement.
- Cybersécurité (Security) : Les systèmes d'IA introduisent de nouveaux risques tels que l'empoisonnement de données, le vol de modèles ou les attaques adversariales.
- Transparence et explicabilité (Transparency and explainability) : L'organisation doit pouvoir expliquer clairement le fonctionnement et les décisions du système d'IA aux parties prenantes.

Comprendre la norme ISO 42001

02

Présentation de la norme ISO 42001 et de la certification

👉 Qu'est-ce que l'ISO 42001 ?

L'ISO 42001 est la première norme internationale dédiée au management de l'intelligence artificielle.
Elle définit un cadre de gouvernance pour les organisations qui conçoivent, développent, déploient ou utilisent des systèmes d'IA.
Son objectif est clair : encadrer, maîtriser et améliorer l'usage de l'IA afin de garantir des pratiques sûres, éthiques et performantes.

Une norme de management avant tout

Comme les autres normes de la famille ISO, la 42001 repose sur la structure HLS (High Level Structure), commune à des référentiels tels que l'ISO 9001 (qualité) ou l'ISO 27001 (sécurité de l'information).
Elle s'intègre donc facilement dans un système de management existant, permettant aux entreprises déjà certifiées d'étendre leur démarche à la gouvernance de l'IA sans tout reconstruire.
L'enjeu : inscrire l'IA dans une logique de management global — avec des objectifs, des indicateurs, des audits et une amélioration continue.

Les exigences clés

La norme demande aux organisations de :

- Définir une politique IA claire alignée sur leurs objectifs stratégiques ;
- Identifier les parties prenantes et leurs attentes (clients, utilisateurs, régulateurs, partenaires) ;
- Mettre en place une évaluation et une maîtrise des risques liés à l'IA ;
- Garantir la sécurité, la fiabilité et la transparence des systèmes IA ;
- Assurer la formation, la communication et la responsabilité des équipes impliquées ;
- Mesurer la performance et améliorer continuellement le dispositif.

Le périmètre d'application

L'ISO 42001 s'applique à tout type d'organisation utilisant ou développant de l'intelligence artificielle :

- Systèmes internes (outils décisionnels, automatisation, RH, cybersécurité, etc.)
- Produits et services IA (logiciels, SaaS, plateformes, solutions embarquées)
- Processus métiers intégrant l'IA (production, analyse, support client, innovation…)

Cette flexibilité permet d'adapter le périmètre à la maturité et aux priorités de chaque entreprise.

La certification ISO 42001

Être certifié ISO 42001 signifie que l'organisation respecte les exigences de la norme et a mis en place un système de management de l'IA (AIMS) efficace.
L'audit est réalisé par un organisme accrédité, sur la base de preuves (politiques, processus, contrôles, registres d'usages).
Cette certification démontre à la fois la maîtrise des risques IA, la conformité réglementaire (AI Act, RGPD, NIS2) et l'engagement dans une démarche responsable et performante.
En résumé, l'ISO 42001 permet de passer de l'expérimentation à la gouvernance, et de transformer l'IA en un véritable levier de confiance et de compétitivité durable.

Les 6 piliers de l'ISO 42001

La norme ISO 42001 repose sur six grands piliers complémentaires.
Ils couvrent à la fois les aspects techniques, organisationnels et éthiques de l'intelligence artificielle, avec un objectif commun : **assurer un usage sûr, maîtrisé et responsable de l'IA.**

1. Gouvernance et responsabilité

Ce pilier définit la structure de pilotage de l'IA dans l'organisation.
L'entreprise doit désigner des rôles clairs (responsable IA, comité de gouvernance, référents métiers) et formaliser ses objectifs, politiques et indicateurs.
La gouvernance permet d'assurer la cohérence entre la stratégie, l'innovation et la maîtrise des risques.
Elle introduit la clarté des rôles : savoir qui décide, qui valide, et comment les impacts de l'IA sont suivis et évalués.
C'est le socle d'un pilotage équilibré entre ambition technologique et responsabilité.

2. Gestion des risques IA

Avant toute chose, le rôle que joue l'organisation dans l'IA — concepteur, intégrateur ou simple utilisateur — est déterminant : il influence la nature des risques à gérer et le niveau de contrôle attendu.
L'ISO 42001 accorde une place centrale à cette gestion des risques.
On recommande de s'appuyer sur les principes de l'ISO/IEC 23894 (gestion du risque spécifique à l'IA), mais aussi sur des cadres reconnus comme l'ISO 27005 (sécurité de l'information) ou le NIST AI Risk Management Framework pour définir votre méthode d'analyse des risques.
Les risques concernent autant les aspects techniques (biais, dérives, perte de contrôle des modèles) que organisationnels (erreurs de décision, atteinte à la réputation, non-conformité).
Les travaux de l'OWASP AI Security and Privacy Guide complètent cette approche en identifiant les menaces propres aux modèles, aux données d'entraînement et aux chaînes MLOps.
Ce pilier vise à rendre les systèmes d'IA prévisibles, sûrs et contrôlables tout au long de leur cycle de vie.

3. La maîtrise de l'IA

La qualité et la sécurité sont indissociables dans le domaine de l'IA.
L'IA repose sur des infrastructures critiques et manipule des volumes massifs de données sensibles.
La norme reprend les principes classiques de la sécurité de l'information — Disponibilité, Intégrité, Confidentialité et Preuve (DICP) — et les étend à la sécurité des modèles eux-mêmes : protection contre la falsification de données d'entraînement, attaques adversariales, vols de modèles ou comportements imprévus. La norme prévoit 11 critères / objectifs que vous pouvez sélectionner pour assurer la maîtrise de votre IA.
L'objectif est d'assurer une IA fiable et robuste, capable de produire des résultats cohérents et auditables, même en cas d'incident ou d'erreur humaine.

Les 6 piliers de l'ISO 42001 (suite)

4. Des processus pour l'éthique et la transparence

La norme promeut une IA explicable, équitable et responsable.
Elle encourage les organisations à établir des processus, documenter leurs modèles, leurs données et leurs processus de décision, afin d'assurer la traçabilité et la compréhension des systèmes par les utilisateurs ou les autorités.
Les travaux de Numeum, notamment sa *Charte d'engagement pour une IA responsable*, vont dans le même sens : garantir que l'IA reste au service de l'humain, respecte la diversité et limite les biais.
Ce pilier relie directement la performance technologique aux valeurs sociétales, en plaçant la transparence et la responsabilité au cœur de la confiance numérique.

5. Conformité réglementaire

Enfin, l'ISO 42001 aide les organisations à anticiper les obligations légales liées à l'usage de l'IA.
Elle s'aligne sur les cadres européens comme l'AI Act, qui classe les systèmes selon leur niveau de risque et impose des exigences de transparence, de documentation et de supervision.
Elle complète également le Cyber Resilience Act (CRA), centré sur la sécurité des produits numériques, ainsi que le RGPD, pour la protection des données personnelles.
Ce pilier fait de l'ISO 42001 un outil de convergence entre gouvernance interne et conformité réglementaire, en offrant un cadre harmonisé à l'échelle européenne.

6. Compétences, culture et amélioration continue

Ce pilier met l'accent sur l'humain et la capacité d'adaptation des organisations face à l'IA.
Il couvre:

- La montée en compétence des collaborateurs (comprendre les modèles, leurs limites et leurs usages)
- La culture IA partagée dans l'entreprise : éthique, expérimentation, collaboration homme–machine
- La formation continue pour suivre l'évolution rapide des outils et des réglementations
- L'amélioration continue des processus IA grâce aux retours d'expérience et aux audits internes

L'objectif : faire de l'IA non pas une technologie isolée, mais un levier collectif de transformation.
C'est la dimension la plus "vivante" du management de l'IA — celle qui ancre la norme dans la réalité quotidienne.

L'ISO 42001 ne se limite pas à réduire les risques : elle permet d'installer une culture de confiance, de responsabilité et de performance autour de l'intelligence artificielle.

Choisir ses objectifs

La logique d'une certification, qu'il s'agisse de l'ISO 27001, 9001 ou 42001, repose sur l'alignement du système de management avec la stratégie et le contexte de l'entreprise.

Autrement dit, il ne s'agit pas d'appliquer des exigences de manière uniforme, mais de construire un système cohérent avec :

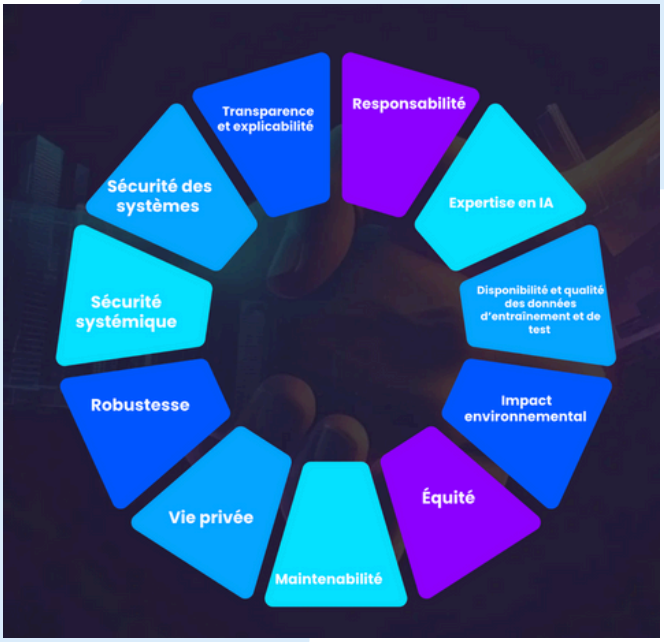
- Le contexte interne et externe de l'organisation (environnement économique, réglementaire, technologique, etc.)
- Les besoins et attentes des parties prenantes (clients, autorités, partenaires, utilisateurs, etc.)
- Les orientations et les objectifs de la direction, qui définissent la vision et les priorités de l'entreprise.

Ainsi, la certification ne vise pas seulement la conformité à une norme, mais l'orientation du management et des processus vers des objectifs mesurables et pertinents pour l'organisation.
C'est ce qui en fait un outil de pilotage stratégique autant qu'un gage de confiance.

L'approche par les risques : un principe clé d'adaptation

L'ISO 42001 repose sur une approche fondée sur les risques, essentielle pour adapter le système de management de l'IA à la réalité de chaque organisation.
Plutôt que d'appliquer mécaniquement toutes les exigences, cette approche permet de proportionner les contrôles et les efforts en fonction du niveau de risque propre à chaque cas d'usage, produit ou service d'IA.
Les organisations peuvent ainsi déterminer le degré de maîtrise nécessaire en tenant compte de leur rôle (concepteur, intégrateur ou utilisateur d'IA), du contexte d'utilisation, de la sensibilité des données traitées et des impacts potentiels pour les individus ou la société.
Cette logique permet d'équilibrer innovation et gouvernance, en concentrant les ressources là où les enjeux sont les plus critiques, tout en préservant la performance et la souplesse du système.
En pratique, cela signifie que le système AIMS n'est pas figé : il évolue en fonction des risques réels et des priorités de l'entreprise, assurant ainsi une conformité intelligente, adaptée et durable.

Le système de management de l'IA doit s'intégrer naturellement dans le fonctionnement global de l'entreprise, au même titre que la qualité ou la sécurité.
La norme ne cherche pas à imposer une méthode unique, mais à fournir un cadre souple pour organiser et piloter les activités liées à l'IA.
Chaque organisation peut s'appuyer sur des référentiels existants (ISO 27001, 9001, 31000, etc.) ou sur sa propre expérience pour structurer la gestion des risques, du cycle de vie des modèles ou de la qualité des données.
L'ensemble s'appuie sur une structure commune aux autres normes ISO, ce qui facilite l'intégration de l'IA dans les systèmes de management déjà en place.



FeelAgile

Qu’est-ce qu’un Système de Management de l’Intelligence Artificielle (SMIA)

Le SMIA (AIMS en anglais) est un système de management qui fournit à l’organisation un cadre pour :

- **Gouverner l’usage, le développement et la fourniture des systèmes d’IA.**
- **Maîtriser les risques spécifiques à l’IA.**
- **Aligner les pratiques avec la stratégie, les valeurs et les objectifs de l’entreprise.**
- **Structurer les processus de management et d’assurance qualité.**
- **Documenter et démontrer la conformité aux exigences internes et réglementaires.**

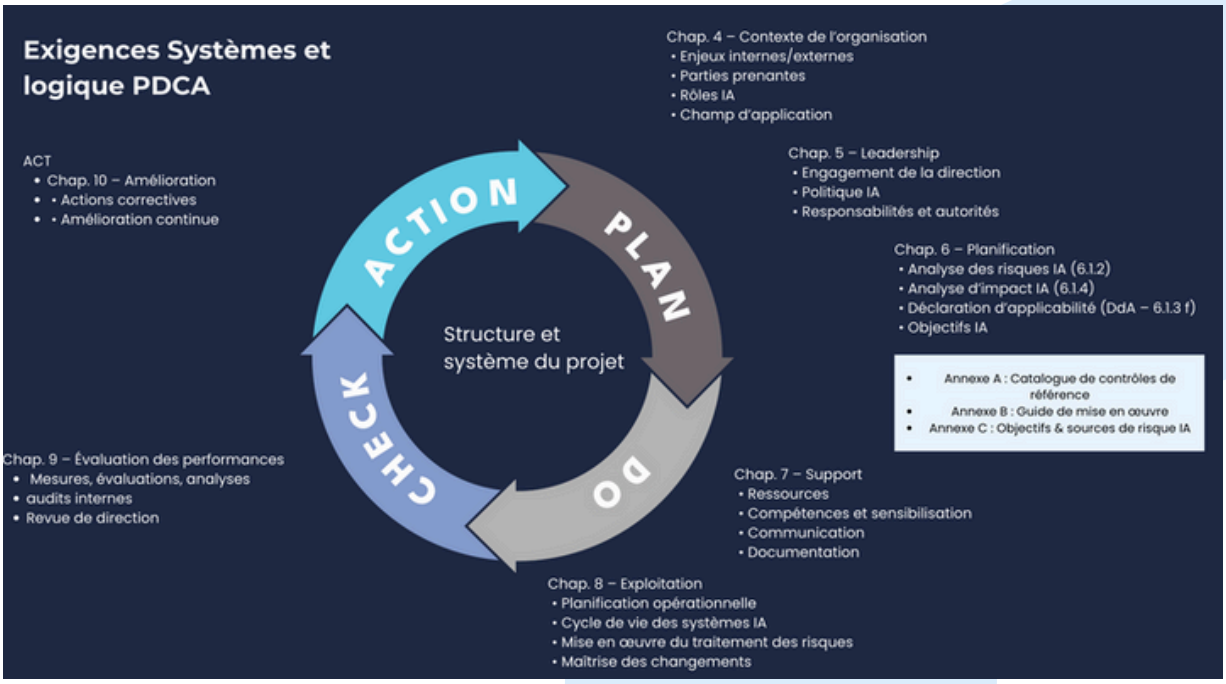
Autrement dit, le SMIA permet de passer d’une IA opportuniste à une **IA maîtrisée et gouvernée**.

Le terme Système de Management couvre les les **processus, objectifs, rôles et ressources** nécessaires au pilotage global de cette technologie.

⚠️ **Erreur fréquente**
Considérer le Système de Management comme un simple ensemble de documents indépendants de l’organisation.

🟢 **Bonne pratique**
Intégrer les processus du SMIA dans ceux déjà existants, selon l’approche processus.
Le SMIA repose sur la logique PDCA (Plan – Do – Check – Act), principe clé des normes ISO. Ce cycle d’amélioration continue permet de structurer, suivre et améliorer la gouvernance de l’IA :

- PLAN : analyser le contexte, les parties prenantes et les risques ; définir les objectifs (éthique, performance, sécurité…).
- DO : déployer les processus nécessaires à la sécurité, à la qualité et au cycle de vie de l’IA.
- CHECK : évaluer les résultats, réaliser des audits et analyser les écarts.
- ACT : ajuster les politiques, objectifs et processus pour s’améliorer en continu.



Et ensuite ?
Cette logique PDCA constitue la base de la norme ISO/IEC 42001, qui définit les exigences d’un SMIA efficace et conforme. Les chapitres suivants détailleront comment déployer cette approche dans votre organisation, de la définition du contexte à la mise en œuvre opérationnelle du système.

ROADMAP

Déployer le SMIA

03

FeelAgile

Votre roadmap projet

La roadmap FeelAgile 42001 est bien plus qu'un simple guide ; c'est une boussole stratégique pour bâtir votre système de management de l'intelligence artificielle (SMIA) en toute confiance. Elle offre une vision claire, structurée et immédiatement actionnable, pour transformer la conformité IA en véritable moteur de création de valeur.
Pas à pas, vous construisez, avec nous, un cadre de gouvernance parfaitement aligné à vos usages, votre gestion des risques et votre niveau de maturité.
Son approche conjugue rigueur, agilité et vision long terme pour faire de votre conformité un avantage concurrentiel durable.

L'objectif ? Faire de vous un acteur de la gouvernance IA, capable non seulement de répondre aux exigences réglementaires, mais surtout d'anticiper, de progresser et de maîtriser vos usages d'intelligence artificielle.

Étape	Explication
1 - Diagnostic et feuille de route	Cette première étape permet de comprendre comment la norme s'applique à votre organisation et d'adapter son cadre à votre contexte spécifique. Elle vise à définir sur quoi vous voulez déployer le SMIA et à établir une feuille de route globale au projet. Cette phase inclut la sensibilisation et la formation initiale.
2 - Cadrage du SMIA (1 mois)	Définir la politique IA, le domaine d'application, les objectifs IA et le dossier de stratégique (enjeux, parties intéressées). Elle vise à clarifier le périmètre et les objectifs du système.
3 - Analyse des risques (1 mois)	Réaliser l'analyse des risques et des impacts, établir le plan de traitement et la déclaration d'applicabilité. Cette étape doit suivre une méthode structurée. Toutes les actions à conduire pour la conformité y sont définies et formalisées.
4. Définition du SMIA (2 à 6 mois)	Élaborer les processus, procédures et modèles du système de management de l'IA. Produire la documentation technique, les plans de tests et les dossiers de conception. Cette phase définit les processus qui vont devoir etre appliqués.
5. Mise en place du SMIA (1 à 3 mois)	Mettre en œuvre les processus et les politiques planifiées. Déployer les formations, les indicateurs (KPI) et les revues internes. L'objectif est de démontrer que tout ce qui a été planifié est effectivement appliqué.
6. Audit blanc (1 semaine)	Réaliser un audit interne complet selon les méthodes ISO. Identifier les écarts et établir un plan d'actions correctives. À ce stade, le SMIA doit être opérationnel et conforme aux exigences de la norme.
7. Préparation audit et revue de direction (3 semaines)	Corriger les écarts identifiés lors de l'audit blanc, conduire la revue de direction et finaliser le plan de préparation à la certification. Cette étape confirme la maturité du système avant l'audit officiel.
8. Audit de certification	Étape finale : l'audit de certification permet de valider la conformité du SMIA et d'obtenir la certification ISO 42001. C'est la reconnaissance officielle de la gouvernance IA mise en place.

Le plan projet

Approche management de projet

La mise en œuvre d'un système de management de l'intelligence artificielle (AIMS) selon la norme ISO 42001:2023 doit être conduite comme un projet structuré, appliquant les principes du management par les risques, de la conformité et de l'amélioration continue (cycle PDCA : Plan – Do – Check – Act).

L'IA constitue une transformation majeure, à la fois technologique et organisationnelle. Sa mise en place requiert une démarche d'entreprise intégrée, alignée avec la stratégie et les objectifs business.

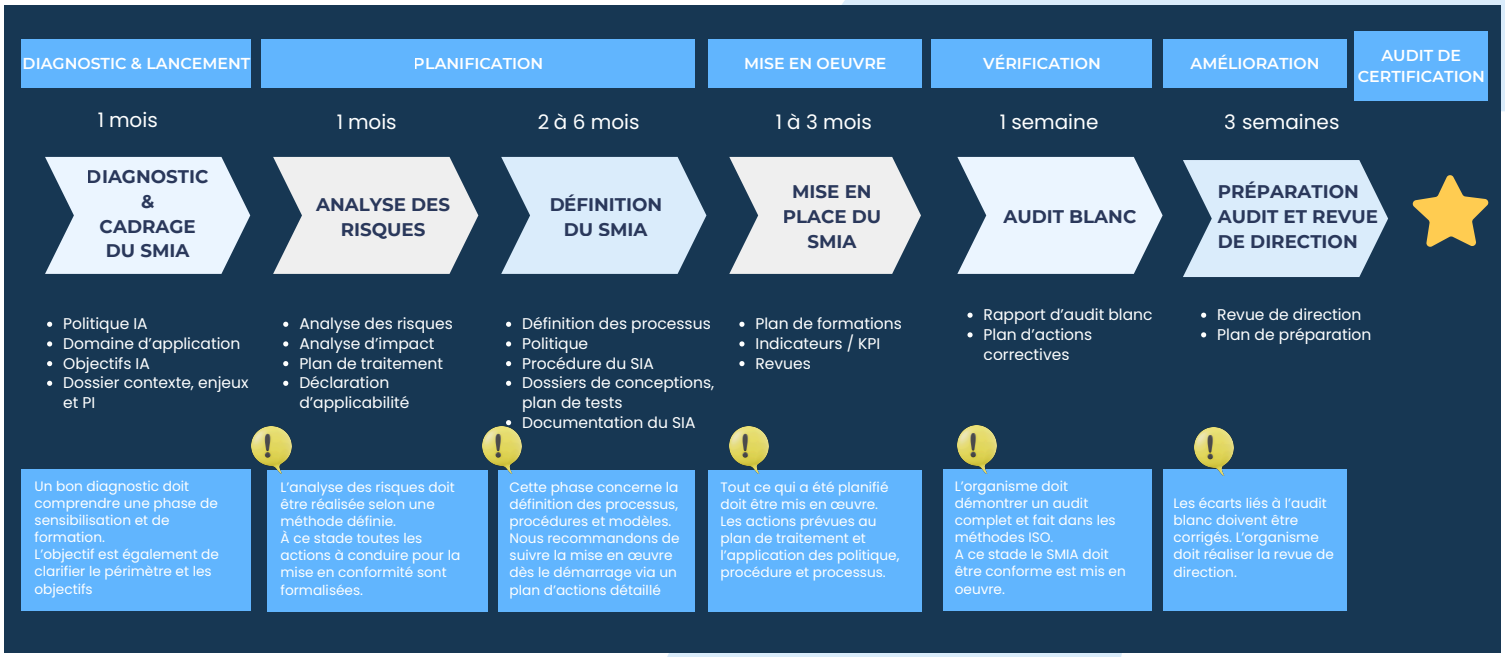
Au-delà de la simple certification, l'enjeu est de bâtir un cadre pérenne de gouvernance, de maîtrise et de confiance des systèmes d'intelligence artificielle, tout en accompagnant la transformation globale vers une utilisation responsable, performante et créatrice de valeur.

Une norme adaptée à la diversité des contextes

La mise en œuvre de l'ISO 42001 doit s'adapter à la variété des contextes organisationnels et des usages de l'intelligence artificielle. Que ce soit pour un outil utilisé en interne, un système intégré à un produit ou une transformation complète du modèle d'entreprise, les exigences varient en complexité et en champ d'action.

L'approche proposée est volontairement flexible : elle offre une méthode universelle, modulable selon la taille de l'organisation, ses activités et ses enjeux. Chaque organisation peut ainsi déployer un management responsable de l'IA, proportionné à son périmètre, tout en respectant ses spécificités et objectifs stratégiques

PLANNING DU PROJET



FeelAgile

ÉTAPE 1 - LE DIAGNOSTIC

Cette étape initiale a pour but de déterminer comment la norme ISO 42001 s'applique à votre organisation et de poser les fondations du futur système de management de l'intelligence artificielle (SMIA).
L'objectif est de définir clairement le périmètre, les enjeux et les objectifs pour adapter la démarche à votre contexte, et préparer une mise en œuvre réaliste et efficace.

Objectif

- Poser les bases du projet ISO 42001 avant son déploiement opérationnel.
- Comprendre la norme et évaluer sa pertinence pour votre entreprise.
- Concevoir une feuille de route adaptée.
- Estimer les ressources nécessaires.
- Définir des hypothèses initiales sur le périmètre et la gouvernance pour la phase de cadrage.

Méthodes

- Entretiens ciblés avec les directions métiers, IT, data, juridique et innovation pour identifier les usages actuels de l'IA.
- Analyse documentaire (politiques existantes, stratégie IA, sécurité, RGPD, qualité).
- Revue des exigences spécifiques à votre organisation.
- Formation à la norme ISO 42001.
- Atelier de cadrage pour formaliser le périmètre du SMIA et définir les objectifs liés à l'IA.

Déroulé

- Phase de sensibilisation : acquisition de la philosophie de la norme et compréhension des exigences clés.
- Diagnostic des pratiques existantes : cartographie des usages IA, identification des forces et faiblesses.
- Définition provisoire du périmètre du SMIA.
- Élaboration d'une feuille de route personnalisée (90 jours, 6 mois, 12 mois).
- Restitution et validation avec la direction : priorisation et recommandations, décision de lancement.

Bénéfices

- Vision claire de la norme ISO 42001 et de son utilité.
- Stratégie partagée avant le lancement du projet.
- Identification initiale des périmètres IA et enjeux prioritaires.
- Feuille de route validée avec un expert.
- Gain de temps et clarté pour la phase de cadrage.

`Livrables

- Compte rendu diagnostic initial résumant contexte et maturité IA.
- Feuille de route détaillée (étapes, jalons, planning).
- Proposition du domaine d'application initial.
- Recommandations expertes pour le cadrage.
- Formations et sensibilisations.

Pour cette étape, nous vous recommandons de faire appel à un expert reconnu tel que FeelAgile.

ÉTAPE 2 - LE LANCEMENT ET CADRAGE

Objectifs

Cette étape marque le point de départ du projet de mise en œuvre du SMIA. Son but est de clarifier le sens et les objectifs de la démarche : pourquoi engager cette mise en conformité, quels résultats attendre, et comment maîtriser les usages de l'IA dans votre organisation.
Elle permet de définir précisément les objectifs, le périmètre et le niveau de gouvernance souhaité, afin d'aligner le système de management sur la stratégie globale et la valeur créée par l'IA.

Réunion de lancement

- Définir l'équipe projet et les responsabilités.
- Établir le planning.
- Présenter les objectifs et la feuille de route issue du diagnostic initial.

Ce moment symbolise le coup d'envoi officiel du projet.

Cartographier les usages de l'IA sur le périmètre que vous voulez prendre en compte

- Identifier toutes les applications IA existantes, qu'elles soient internes (outils, automatisations, prises de décision) ou externes (solutions SaaS, API IA).
- Distinguer les cas d'usage expérimentaux de ceux en production.
- Clarifier les rôles des parties prenantes vis-à-vis de l'IA (développeur, fournisseur, utilisateur).
- Délimiter le périmètre précis de la démarche.

Analyser le contexte et les parties prenantes

- Identifier les enjeux internes et externes liés à l'IA : innovation, réputation, conformité, dépendance technologique.
- Recenser les parties prenantes internes et externes ainsi que leurs attentes.
- Examiner les exigences réglementaires, du marché et des utilisateurs.

Formaliser le domaine d'application du SMIA

Ce document définit le périmètre précis d'application du système ISO 42001 dans l'entreprise :

- Définir le champ d'application de la certification IA (projets, produits, processus).
- Clarifier les responsabilités : qui pilote quoi, qui agit sur quoi.
- Décrire le domaine d'application en termes de processus, structures organisationnelles et périmètres technologiques.

Déterminer les objectifs et rédiger la politique

Une fois le périmètre et les systèmes d'IA identifiés :

- Définir des objectifs mesurables, alignés avec les enjeux identifiés (ex. : réduire de 20% le taux d'erreur des modèles, documenter 100% des cas d'usage critiques).
- Identifier les améliorations visées.
- Rédiger la politique IA, en cohérence avec la stratégie globale et les politiques existantes (sécurité, qualité, conformité).

ÉTAPE 3 - ANALYSE DES RISQUES

Analyse des risques : un pilier essentiel du SMIA
L'analyse des risques est au cœur du système de management de l'intelligence artificielle (SMIA). Elle permet de comprendre, prioriser et maîtriser les risques techniques, éthiques, juridiques ou organisationnels liés à l'IA. Cette démarche ciblée adapte la gouvernance à la criticité de chaque usage et révèle les vulnérabilités telles que biais, erreurs, manque de transparence, failles de sécurité ou atteintes à la réputation.

Objectifs de l'analyse des risques
- Sur le plan opérationnel, renforcer la fiabilité et la sécurité des systèmes d'IA.
- Sur le plan stratégique, fournir une base objective pour orienter les décisions, prioriser les investissements et démontrer la conformité aux réglementations (AI Act, RGPD, ISO 42001).

En résumé, l'analyse des risques structure et maîtrise la gestion de l'IA, garantissant une innovation alignée avec les objectifs de l'entreprise.

Méthodologie recommandée
- Choisir la méthode adaptée aux risques techniques, éthiques ou réglementaires selon les priorités.
- Documenter la méthode pour assurer la reproductibilité et le suivi.
- Utiliser une matrice spécifiquement conçue pour les risques liés à l'IA (biais, sécurité, transparence).

Conseil : solliciter un expert pour définir une approche robuste et adaptée.

Mise en œuvre de l'analyse des risques IA
- Recenser les actifs et usages IA.
- Réaliser l'analyse et l'évaluation des risques.
- Élaborer le plan de traitement (processus, contrôles, documentation).
- Valider le plan d'actions et la déclaration d'applicabilité (SoA), puis assurer son suivi.

Le plan de traitement est une étape stratégique déterminant les processus, documents et contrôles nécessaires au système.

Validation du plan de traitement
- Vérifier que les contrôles pertinents de l'annexe A sont bien pris en compte au regard des risques.
- Rédiger une déclaration d'applicabilité (SoA) justifiant les contrôles retenus et leur mise en œuvre.
- Finaliser le plan d'actions, validé par la direction.

Évaluation des impacts et suivi
- Intégrer une évaluation systématique des impacts sociétaux (vie privée, équité, effets humains) dans chaque projet IA.
- Actualiser cette évaluation lors de tout changement significatif.
- Définir et suivre des indicateurs-clés pour mesurer les progrès et améliorer continuellement.

ÉTAPE 4 - DÉFINITION DU SMIA

Objectif de cette phase

Cette phase a pour but de traduire les résultats de l'analyse des risques en exigences opérationnelles et d'intégrer les contrôles dans les processus du cycle de vie des systèmes d'IA. Toutes les actions (documents, processus, etc.) sont planifiées, mais doivent encore être précisément définies et mises en œuvre.

Durant cette étape, vous rédigerez les processus, politiques et procédures. Pour cela, vous vous appuierez sur l'expertise interne et externe, ainsi que sur les bonnes pratiques des annexes A et B de la norme, et d'autres référentiels sectoriels tels que NIST ou OWASP.

Chaque document devra suivre un circuit de validation strict. Les actions à mettre en œuvre pour chacun doivent être identifiées et planifiées.

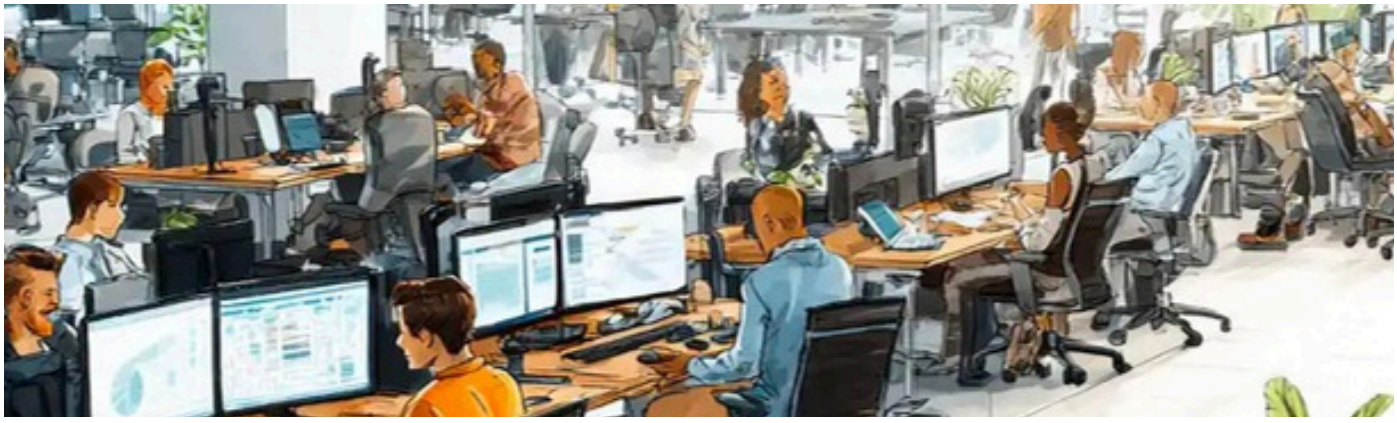
Livrables attendus :

Selon l'analyse des risques et votre périmètre, les livrables peuvent inclure :

- Catalogue des contrôles IA retenus (techniques, organisationnels, éthiques).
- Politiques IA (données, RGPD, etc.).
- Processus métiers : conception, validation, mise en production des systèmes d'IA.
- Processus SMIA : gestion des incidents, documentation, etc.
- Dossiers de validation et de tests des modèles.
- Description des fonctionnement et limites des systèmes IA.

Actions dans l'organisation

- Rédiger et appliquer les politiques, processus et procédures.
- Définir les outils et solutions pour maîtriser les systèmes d'IA.
- Communiquer les mesures de gouvernance et sécurité dans les processus existants.
- Documenter la traçabilité des modèles et des données.
- Définir les points de supervision humaine et de revue de conformité.



ÉTAPE 5 - MISE EN OEUVRE DU SMIA

Objectif de cette phase

Le déploiement du Système de Management de l'Intelligence Artificielle (SMIA) consiste à mettre en œuvre concrètement les processus, politiques et contrôles définis lors de la phase de conception.
Cette étape marque le passage de la planification à l'action. Elle vise à intégrer la gouvernance de l'IA dans le quotidien de l'organisation, en veillant à ce que chaque acteur comprenne son rôle, ses responsabilités et les bonnes pratiques à adopter.

Le déploiement comprend la mise en place des politiques IA, ainsi que le déploiement des contrôles techniques et organisationnels nécessaires pour assurer conformité et fiabilité.
Les équipes sont formées et accompagnées pour s'approprier les processus, comprendre la logique de la norme et garantir la cohérence des actions sur l'ensemble du périmètre.
Cette phase assure aussi la traçabilité des activités, la collecte des preuves de conformité et favorise la montée en compétence progressive des équipes.

N'oubliez pas que parmi ces preuves figurent les indicateurs de performance du SMIA.L'objectif final est de disposer d'un système vivant et opérationnel capable de démontrer la maîtrise des usages de l'IA, de sécuriser les décisions automatisées et de soutenir l'amélioration continue.

Accompagnement des équipes

- Formations et sensibilisation : organiser des sessions ciblées pour présenter les principes du SMIA, les exigences ISO 42001 et les bonnes pratiques d'usage de l'IA. (Plan et registre des formations réalisées)
- Déploiement des outils associés : mettre à disposition les supports, registres, tableaux de bord et plateformes nécessaires au suivi du système.
- Explication des processus : clarifier le rôle de chaque acteur, les étapes clés et les liens entre les processus (gouvernance, risques, données, usage responsable, etc.).

Pilotage

- Suivi des actions : animer la mise en œuvre opérationnelle, identifier les points de blocage et ajuster les priorités selon l'avancement (registre de suivi des actions de mise en œuvre).
- Suivi des processus de validation : vérifier la bonne application des procédures, le traitement des documents, les revues de changement et la conformité des pratiques (procédures et modes opératoires validés et diffusés).

Preuves et indicateurs

- Production des preuves : s'assurer que chaque activité du SMIA génère les éléments de preuve nécessaires (enregistrements, rapports, logs, validations).
- Suivi des indicateurs : collecter et analyser les indicateurs de performance et de conformité pour mesurer l'efficacité du système et alimenter la revue de direction.

ÉTAPE 6 - AUDIT BLANC

Objectif de cette phase

L'audit blanc constitue une répétition générale avant l'audit de certification. Il permet de vérifier que le système de management de l'intelligence artificielle (SMIA) est correctement déployé, compris et appliqué par toutes les équipes.

Réalisé par un auditeur interne ou un expert externe, cet audit évalue la conformité aux exigences de la norme ISO 42001, l'efficacité des processus, la traçabilité des actions et la qualité des preuves fournies.

Cette phase a pour but d'identifier les écarts (non-conformités, axes d'amélioration, points faibles) et de mettre en place un plan d'actions correctives avant la revue de direction. L'objectif est de garantir que le SMIA soit fiable, opérationnel et prêt pour l'audit officiel.

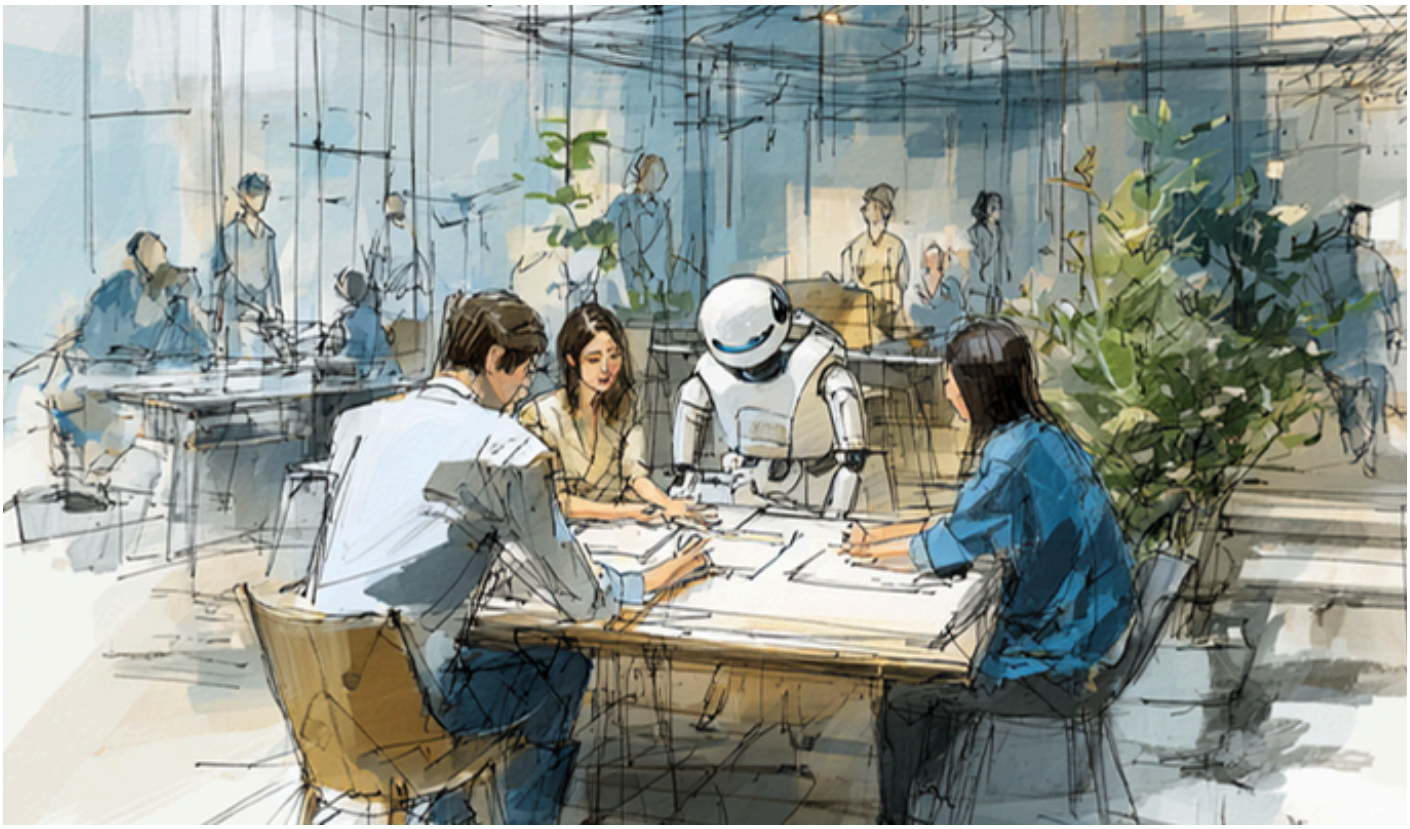
Obligations

- Les audits blancs ISO 42001 doivent être conduits par des auditeurs qualifiés et externes au périmètre audité.
- Les audits doivent être complets et porter sur l'ensemble du système de management

Actions correctives

L'objectif de cet audit est :

- De préparer les équipes à l'audit de certification
- D'identifier et traiter tous les écarts subsistants du SMIA.



ÉTAPE 7 - REVUE DE DIRECTION (1/2)

Objectif de cette phase

La revue de direction constitue la dernière étape du cycle de mise en œuvre avant la certification.
Elle a pour but d'évaluer la performance globale du SMIA, sur la base des audits, des indicateurs, des retours d'expérience et des actions correctives mises en place.

La direction examine la pertinence du périmètre, des objectifs et des ressources allouées, puis décide des axes d'amélioration ou d'évolution du système.

Cette revue matérialise l'engagement du top management et démontre que la gouvernance IA est pilotée au plus haut niveau.

Elle clôture le cycle PDCA (Plan – Do – Check – Act) et permet d'aborder l'audit de certification dans une démarche de maîtrise et de confiance.

Objectif de cette phase

Vérifier la performance, la conformité et l'efficacité du système de management et des contrôles mis en œuvre.

Livrables attendus :

- Rapport de revue de direction, réalisé après l'audit interne, synthétisant les résultats et décisions clés.

ÉTAPE 7 - PRÉPARATION DE L'AUDIT DE CERTIFICATION ET AMÉLIORATION (2/2)

Objectif de cette phase

Assurer la pérennité, la conformité et la performance du système de management de l'IA (AIMS) par une démarche d'amélioration continue.

Cette phase vise à consolider les pratiques, corriger les écarts identifiés lors des audits internes ou des audits blancs, et préparer l'organisation à la certification ISO 42001.

Elle symbolise la transition d'un projet de mise en place vers un fonctionnement opérationnel durable et maîtrisé.

Livrables attendus :

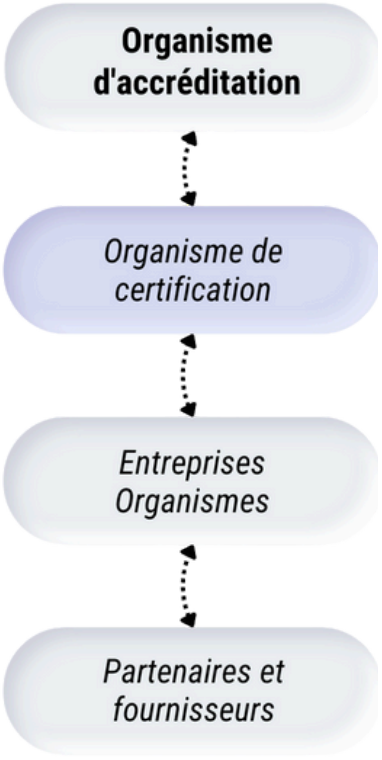
- Registre des non-conformités (NC) et actions correctives associées
- Plan d'amélioration continue consolidé (actions, responsables, échéances, résultats)
- Comptes rendus des audits internes et des audits blancs
- Checklist de préparation à la certification ISO 42001
- Plan et rapport de formation continue pour la montée en compétence des équipes
- Compte rendu de revue finale de direction préalable à la certification

Actions à mener

- Mettre en place une gestion rigoureuse et structurée des non-conformités.
- Définir et formaliser la notion de non-conformité adaptée à l'organisation.
- Constituer et maintenir un registre des non-conformités avec suivi régulier.
- Organiser des séances de préparation pour rappeler les points critiques et lever les non-conformités majeures identifiées lors de l'audit blanc.

Cette phase est cruciale pour assurer la levée efficace des non-conformités majeures et garantir une préparation optimale à la certification.

Certification ISO 42001 : critères, audits et accréditation



Importance d'un organisme accrédité pour la certification ISO 42001

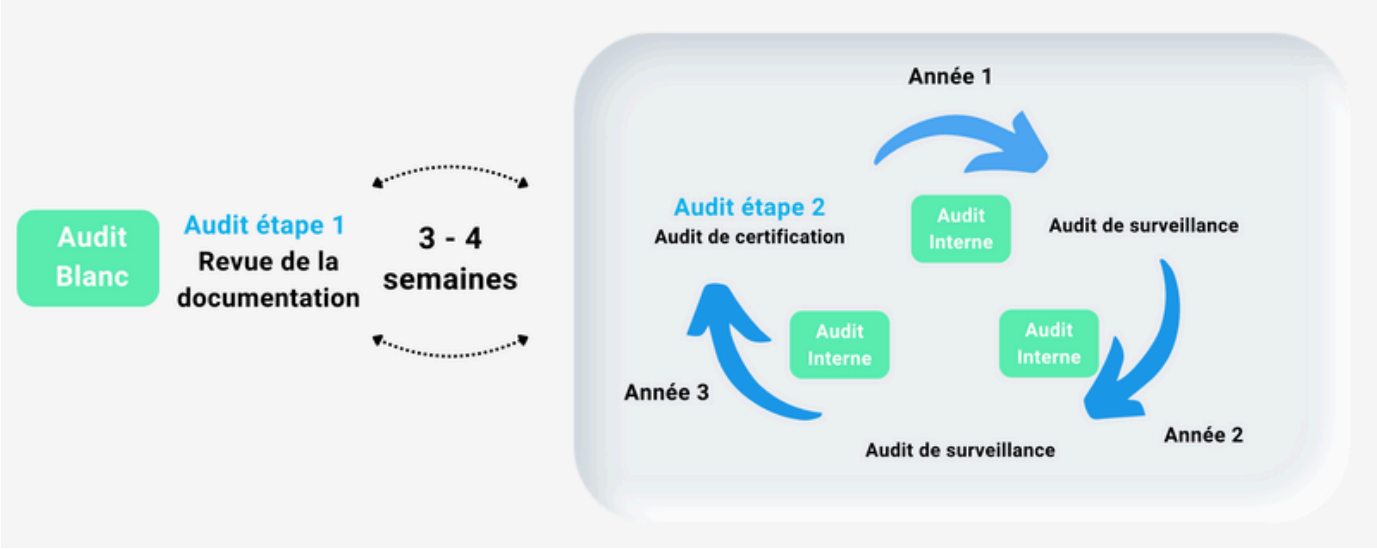
Une certification ISO 42001 n'a de valeur que si elle est délivrée par un organisme accrédité.
C'est la garantie que votre démarche est sérieuse, reconnue, et alignée avec les attentes des clients, partenaires et régulateurs

Qu'est-ce qu'un organisme accrédité ?

Un organisme de certification accrédité est un organisme qui a été évalué et reconnu officiellement (en France, par le Cofrac, à l'international par des équivalents comme UKAS, DAkkS, etc.) pour :

- sa compétence technique,
- sa rigueur dans les audits,
- sa conformité aux exigences ISO 17021 (norme encadrant les organismes certificateurs).

La certification ISO 42001 est délivrée pour une durée de 3 ans, avec un audit initial complet, suivi de deux audits de surveillance annuels pour vérifier le maintien et l'amélioration continue du système.
Au terme des 3 ans, un audit de renouvellement est réalisé pour prolonger la certification.



EXIGENCES

Le référentiel ISO 42001

04

PRÉSENTATION DU RÉFÉRENTIEL ET DES EXIGENCES DE L'ISO 42001

L'ISO 42001 est le premier référentiel international dédié au management de l'intelligence artificielle.
Il définit les exigences organisationnelles qu'une entreprise doit mettre en place pour gouverner, maîtriser et améliorer l'usage de l'IA, dans une logique de confiance, de performance et de responsabilité.

La norme ne cherche pas à encadrer la technologie, mais à organiser la manière dont une organisation pilote ses systèmes et usages d'IA.

L'ISO 42001 s'inscrit dans la continuité des grandes normes de management (ISO 9001, ISO 27001) avec lesquelles elle partage la structure harmonisée (HLS – High Level Structure).
Cette structure commune facilite son intégration dans un système déjà existant et favorise une gouvernance globale.

Elle repose sur le cycle d'amélioration continue (PDCA : Plan, Do, Check, Act), garantissant que le système d'IA reste cohérent, performant et évolutif dans le temps.

La norme s'articule autour de sept chapitre d'exigences formant la structure du Système de Management de l'IA (SMIA) :

- **Chapitre 4 – Contexte de l'organisation**
  - Déterminer les enjeux internes et externes, les parties prenantes et le périmètre d'application du SMIA.
- **Chapitre 5 – Leadership**
  - Définir la gouvernance IA, les rôles, les responsabilités et la politique IA.
- **Chapitre 6 – Planification**
  - Identifier les risques et opportunités liés à l'IA, planifier les actions et fixer les objectifs du système.
- **Chapitre 7 – Support**
  - Définir les ressources nécessaires : compétences, communication, documentation et gestion des informations.
- **Chapitre 8 – Opération**
  - Déployer les processus liés au cycle de vie de l'IA : conception, développement, validation, surveillance et amélioration.
- **Chapitre 9 – Évaluation des performances**
  - Mesurer l'efficacité du système, conduire des audits internes et suivre les indicateurs.
- **Chapitre 10 – Amélioration**
  - Identifier les écarts, traiter les non-conformités et renforcer en continu la maturité du système.

Les annexes : un complément essentiel aux exigences
Les annexes A et B de la norme complètent les exigences des chapitres principaux en proposant des contrôles, bonnes pratiques et éléments d'application.
Elles ne sont pas auditées directement, mais servent de référentiel de référence pour la mise en œuvre et la déclaration d'applicabilité du SMIA :

- Annexe A – Contrôles et objectifs associés : liste des contrôles possibles pour répondre aux exigences de la norme (gouvernance, données, sécurité, supervision, transparence, etc.).
- Annexe B – Lignes directrices d'application : explications et exemples illustrant comment adapter les contrôles selon le contexte, le rôle de l'organisation et le niveau de risque.

Ces annexes constituent un socle opérationnel permettant d'assurer la cohérence et la traçabilité du système. Elles sont indispensables à la préparation de la déclaration d'applicabilité (SoA – Statement of Applicability), document clé du SMIA.

CHAPITRE 4 - CONTEXTE DE L'ORGANISME

La première étape d'un système de management de l'IA consiste à comprendre le contexte dans lequel l'organisation évolue et à définir les objectifs du système.
La clause 4 de l'ISO 42001 rappelle que tout projet IA doit être ancré dans le contexte de l'organisation. Elle exige d'identifier les enjeux internes et externes, les attentes des parties prenantes et la finalité des systèmes d'IA développés ou utilisés.
L'organisation doit clarifier son rôle (développeur, fournisseur, utilisateur, superviseur) et déterminer le champ d'application de son système de management de l'IA.

La norme ISO 42001 exige d'identifier :

- Les enjeux internes et externes (technologiques, réglementaires, éthiques, concurrentiels) ayant un impact sur les usages de l'IA ;
- Les parties prenantes et leurs attentes : clients, utilisateurs, partenaires, autorités, collaborateurs, etc.
- Le périmètre du système de Management de l'IA : quelles activités, produits, services ou processus incluent de l'IA
- Les objectifs stratégiques associés à l'IA : performance, sécurité, conformité, innovation, confiance.

Cette étape permet de poser les bases d'un système cohérent, aligné sur la stratégie de l'entreprise, plutôt qu'un simple ensemble de procédures.
Cette approche vise à garantir que l'IA n'est pas déployée de façon isolée, mais qu'elle est alignée sur les objectifs stratégiques, la gouvernance, les contraintes réglementaires et les dynamiques de marché.
L'organisme est libre de choisir son champ d'application.

CHAPITRE 5 - LEADERSHIP

Le chapitre 5 de la norme ISO 42001 traite du rôle de la direction et de la gouvernance dans la mise en place et le pilotage du Système de Management de l'Intelligence Artificielle (SMIA).
Il repose sur un principe simple, mais essentiel : aucun système de management ne peut réussir sans un engagement réel de la direction et une répartition claire des responsabilités.
Ce chapitre définit les exigences qui garantissent que la gouvernance de l'IA soit cohérente, incarnée et pilotée au plus haut niveau de l'organisation.

La direction doit :

- S'impliquer activement dans le système de management de l'IA (SMIA) et lui donner les ressources nécessaires.
- Définir une politique IA alignée sur la stratégie de l'organisation, intégrant conformité, éthique et amélioration continue.
- Attribuer clairement les rôles et responsabilités, notamment un responsable chargé de suivre la performance du système et d'en rendre compte.

Informations documentées requises :

- Politique IA (obligatoire)
- Description des rôles et des responsabilités (obligatoire)

CHAPITRE 6 - PLANIFICATION

Ce chapitre traite de l'analyse des risques. Cette analyse va vous servir à prioriser les processus et contrôles à mettre en œuvre.

L'organisation doit planifier son système de management de l'IA (SMIA) en :

- Identifiant les risques et opportunités liés à l'IA
- Évaluant et traitant ces risques selon des critères clairs et documentés.
- **Réalisation d'évaluations d'impact IA** sur les individus, les groupes ou la société (à la différence de l'analyse des risques, l'évaluation d'impact porte sur les impacts sociétaux de l'IA)
- Définissant des objectifs IA mesurables cohérents avec la politique
- Planifiant les changements de manière maîtrisée

Informations documentées requises :

- Processus d'évaluation et de traitement des risques IA
- Résultats d'analyses et plans de traitement
- Objectifs IA et plans d'action associés
- Résultats d'évaluations d'impact IA
- Déclaration d'applicabilité

CHAPITRE 7 - RESSOURCES

L'organisation doit fournir les ressources, compétences et informations nécessaires au bon fonctionnement de son système de management de l'IA (SMIA). La direction doit s'assurer que les ressources sont bien disponibles

Elle doit :

- Mettre à disposition les ressources humaines, techniques et financières (7.1).
- Garantir la compétence du personnel impliqué (7.2).
- Assurer la sensibilisation aux enjeux de l'IA (7.3).
- Définir une stratégie de communication interne et externe (7.4).
- Créer, mettre à jour et maîtriser la documentation du système (7.5).

Informations documentées requises :

- Preuves de compétences (CV, formations, habilitations)
- Registre des ressources IA (humaines, matérielles, données, outils)
- Procédure de gestion documentaire
- Politique et plan de communication

CHAPITRE 8 - OPÉRATIONS

Le chapitre 8 décrit la mise en œuvre opérationnelle du système de management de l'IA. Il s'agit simplement de la mise en œuvre des processus et du maintien à jour des analyses de risques.

L'organisation doit :

- Planifier, mettre en œuvre et contrôler les processus IA pour atteindre les résultats attendus.
- Réaliser des analyses de risques IA à intervalles planifiés et à chaque changement significatif.
- Mettre en œuvre les plans de traitement des risques et vérifier leur efficacité.
- Réaliser des évaluations d'impact IA sur les individus, groupes et sociétés.

Informations documentées requises :

- Plans opérationnels IA
- Résultats des analyses et des traitements de risques
- Résultats des évaluations d'impact
- Preuves de surveillance et de mise à jour des processus

CHAPITRE 9 - ÉVALUATION DE LA PERFORMANCE

L'organisation doit évaluer l'efficacité et la performance de son système de management de l'IA. Il s'agit de suivre des indicateurs ou de faire des revues des risques, processus, documents.

Cela comprend :

- Mesurer, analyser et évaluer en continu le fonctionnement du système et les résultats liés à l'IA.
- Réaliser des audits internes planifiés pour contrôler la conformité et l'efficacité du système.
- Organiser des revues de direction périodiques pour garantir la pertinence, l'adéquation et la performance du système.

Informations documentées requises :

- Résultats des suivis, mesures et évaluations.
- Programme et rapports d'audit interne
- Comptes rendus et décisions issus des revues de direction

CHAPITRE 10 - AMÉLIORATION

La clause 10 impose à l'organisation de surveiller, analyser et améliorer en continu l'efficacité de son **système de management de l'intelligence artificielle (SMIA)**

Lorsqu'une non-conformité est détectée (incident, défaillance de modèle, non-respect d'une exigence interne ou réglementaire), l'organisation doit :

- Réagir sans délai pour corriger la non-conformité et en limiter les conséquences.
- Analyser les causes profondes afin d'éviter toute récurrence.
- Mettre en œuvre des actions correctives adaptées et en vérifier l'efficacité.
- Documenter rigoureusement les résultats et décisions prises.

Le système doit être en amélioration permanente, reposant sur les résultats des audits, des revues de direction, des analyses de risques, des incidents et des retours d'expérience.

Cette démarche vise à renforcer la conformité, la performance, la confiance et la maîtrise des risques liés à l'IA, assurant ainsi un alignement continu avec les objectifs stratégiques de l'organisation.

CONCLUSION

Les clauses des chapitres 4 à 10 de la norme ISO 42001 sont strictement obligatoires et ne peuvent en aucun cas être exclues. Ces chapitres définissent le cadre du système de management pour l'intelligence artificielle.

En revanche, les exigences de l'annexe A, qui listent les processus et contrôles à mettre en place, peuvent faire l'objet d'exclusions selon l'analyse des risques et le champ d'application spécifique à votre organisation.

Il est impératif, dans le domaine de l'IA et pour garantir la conformité à cette norme, de s'appuyer également sur les standards techniques et organisationnels du marché ainsi que sur les réglementations en vigueur.

LES ANNEXES

Les annexes de la norme ISO 42001 complètent les exigences principales (chapitres 4 à 10) en fournissant des lignes directrices et des contrôles de référence pour la mise en œuvre du système de management de l'intelligence artificielle.

L'**annexe A** liste les contrôles et objectifs associés, couvrant des domaines clés tels que la gouvernance, la gestion des données, la sécurité, la transparence et la supervision humaine. Elle sert de base à la déclaration d'applicabilité **(SoA),** qui recense les contrôles pertinents pour chaque organisation.

L'**annexe B** détaille chaque objectif de l'Annexe A en proposant des orientations pratiques et des exemples d'application, facilitant l'adaptation des contrôles selon le rôle, le contexte et le niveau de risque.

Les **annexes B, C et D** ne sont pas auditées directement, mais constituent un support essentiel pour démontrer la cohérence, la traçabilité et la maturité du système de management.

Annexe	Type	Titre / Contenu	Rôle et utilité concrète dans le projet 42001
Annexe A	**Normative**	**Reference control objectives and controls** (Objectifs de contrôle et contrôles de référence)	Liste des objectifs et contrôles IA à mettre en place : base de la Déclaration d'Applicabilité (SoA)
Annexe B	**Normative**	**Implementation guidance for AI controls** (Lignes directrices de mise en œuvre des contrôles)	Bonnes pratiques et méthodes pour implémenter les contrôles d'Annexe A, support pour l'audit
Annexe C	**Informative**	**Potential AI-related organizational objectives and risk sources** (Objectifs organisationnels et sources de risques liés à l'IA)	Cartographie des objectifs organisationnels et risques IA : alimente le registre des risques
Annexe D	**Informative**	**Examples of AI domains and applications** (Exemples de domaines et applications de l'IA)	Exemples de domaines d'application IA pour adapter périmètre et contrôles selon le secteur
Annexe D	**Informative**	**Correspondence with other standards** (Correspondance avec d'autres normes de management)	Mapping avec autres normes : facilite intégration et mutualisation documentaire pour sociétés certifiées

Fiches pratiques

05

Fiche pratique – IA Act et ISO 42001

Résumé réglementaire : qu'est-ce que l'IA Act ?
Le Règlement (UE) 2024/1689, appelé IA Act, établit un cadre juridique européen harmonisé pour le développement, la mise sur le marché, le déploiement et l'utilisation des systèmes d'intelligence artificielle (IA) dans l'Union européenne. La conformité à ce règlement est indispensable dans le cadre d'un audit ISO 4200

Objectifs du texte :
- Garantir une IA digne de confiance, centrée sur l'humain et conforme aux droits fondamentaux.
- Fixer des obligations différenciées selon le niveau de risque du système d'IA.
- Éviter la fragmentation réglementaire du marché intérieur européen.
- Favoriser l'innovation tout en assurant transparence, sécurité, traçabilité et surveillance humaine.

Principaux mécanismes :
- Classification des systèmes d'IA selon 4 niveaux de risque : *inacceptable, élevé, limité, minimal.*
- Obligations spécifiques pour les systèmes à haut risque : évaluation de conformité, gestion des données, surveillance humaine, documentation technique, registres d'événements, etc.
- Régime spécifique pour les modèles de fondation (notamment génératifs).
- Supervision par des autorités nationales compétentes et le Comité européen de l'IA.

Articulation avec ISO42001 : cohérence et complémentarité
La norme ISO 42001:2023 est volontaire et définit un système de management de l'IA (SMIA) basé sur le cycle PDCA (Plan – Do – Check – Act). Elle garantit une gouvernance responsable, sécurisée et éthique, et constitue un excellent moyen d'assurer la conformité au IA Act.

Complémentarité
- ISO 42001 permet de structurer la conformité à l'IA Act dans un cadre de management auditable.
- L'IA Act fixe les exigences légales et le processus à respecter (particulièrement pour les systèmes à haut risque).
- L'AIMS (AI Management System) devient un levier opérationnel de conformité réglementaire, démontrant la maîtrise du cycle de vie de l'IA.

Utilisation du IA Act dans une certification ISO 42001 : Il est indispensable d'intégrer les exigences réglementaires dans votre SMIA.

Etape	A faire dans les cadre de l'ISO 42001
Analyse du contexte	• Définir le cadre réglementaire • Inclure l'IA Act dans l'analyse des exigences externes • Identifier les cas d'usage et systèmes concernés par le règlement • Cartographier les exigences applicables
Analyse des risques	• Prendre en compte dans le management des risques IA (identifier des risques règlementaires) • Tracer les mesures de conformité dans la déclaration d'applicabilité • Documenter les contrôles mis en œuvre pour respecter les articles du règlement • Justifier l'exclusion de certaines exigences (si non applicables)
Déploiement	• Intégrer les obligations réglementaires dans les politiques de gestion des données, supervision humaine, transparence, etc. (les références sont importantes)
Vérification	• Auditer la conformité au règlement dans les audits internes • Vérifier que les systèmes couverts respectent les obligations de l'IA Act • En plus de l'IA ACT vous devez vous assurer de la confofmité à l'ensemble des règlementaitons sur les données (RGPD, CRA pour les éditeurs de logiciels, ...)

Fiche pratique - Les rôles de l'IA

Nous recommandons de commencer par étudier la réglementation afin de bien comprendre les rôles liés à l'intelligence artificielle et d'identifier ainsi les responsabilités spécifiques de l'organisation.

Ensuite, cette base pourra être enrichie avec des rôles plus opérationnels, tirés de normes reconnues telles que NIST et ISO.

Ces rôles définissent les obligations légales incontournables et doivent impérativement être intégrés dans le cadre de votre certification.

Voici quelques exemples illustratifs :

Rôle	Définition légale	Responsabilités principales (exemples)
Fournisseur (Provider)	Développe un système d'IA ou le fait développer et le met sur le marché ou le met en service sous son nom ou sa marque.	- Garantir la conformité du système avant mise sur le marché. - Tenir à jour la documentation technique - Mettre en œuvre un système de management du risque - Assurer la surveillance post-commercialisation - Notifier les incidents graves
Déployeur (Deployer)	Utilise un système d'IA sous sa propre autorité.	- Assurer une utilisation conforme à la destination prévue - Mettre en place une supervision humaine effective - Informer les personnes concernées lorsqu'elles interagissent avec un système d'IA - Tenir un registre des activités d'utilisation pour les systèmes à haut risque. - Garantir le respect du RGPD si traitement de données personnelles.
Mandataire (Authorised Representative)	Toute personne physique ou morale établie dans l'Union ayant reçu du fournisseur (souvent non-UE) un mandat écrit pour agir en son nom concernant ses obligations.	- Être le point de contact officiel entre le fournisseur hors UE et les autorités de surveillance. - Conserver la documentation technique et la déclaration de conformité CE. - Coopérer avec les autorités de surveillance ou d'enquête (art. 25).
Importateur (Importer)	Personne physique ou morale établie dans l'UE qui met sur le marché un système d'IA provenant d'un pays tiers.	- Vérifier que le fournisseur a effectué la procédure de conformité CE. - Vérifier la présence du marquage CE et de la documentation technique. - S'assurer que le système est accompagné des informations et instructions requises (art. 26). - Tenir un registre des non-conformités. - Coopérer avec les autorités nationales.
Distributeur (Distributor)	Personne physique ou morale mettant à disposition sur le marché un système d'IA, sans en être le fournisseur ni l'importateur.	- Vérifier que le système porte le marquage CE et dispose des instructions requises. - Ne pas altérer la conformité (ex. par modification logicielle non autorisée). - Suspendre la mise sur le marché en cas de suspicion de non-conformité. - Coopérer avec les autorités compétentes (art. 27).

Fiche pratique - Les objectifs d'IA

Comprendre la notion d'« objectif » dans ISO 42001
Un objectif est un résultat à atteindre, traduisant ce que l'organisation souhaite obtenir grâce à l'intelligence artificielle (IA). Les objectifs permettent de donner une direction, piloter les actions, mesurer les progrès et vérifier que le système atteint les résultats souhaités. Ils doivent être :

- Cohérents avec la politique d'IA de l'organisation
- Mesurables autant que possible (indicateurs, KPI…)
- Révisés régulièrement (cf. § 6.2 de la norme)

Les objectifs peuvent prendre la forme :

- de KPI à atteindre
- d'actions ou projets spécifiques
- de résultats ou performances mesurables

Différents types et niveaux d'objectifs

Niveau	Rôle	Exemple
Stratégiques	Direction générale fixée par la direction	Renforcer la confiance client via la transparence algorithmique
Tactiques	Priorités à moyen terme, pilotées par les équipes management	Mettre en place l'évaluation éthique des usages d'IA
Opérationnels	Concrets, mesurables, appliqués aux activités quotidiennes	Documenter 100% du système "X1" avant fin d'année

- Objectifs d'IA : ce que l'organisation veut atteindre grâce à l'IA
- Objectifs du système de management : ex : taux de conformité, nombre d'audits/écarts
- Objectifs des processus/contrôles : déployés sur des activités ou actions précises

Bonnes pratiques pour formuler un objectif d'IA
Un bon objectif doit être :

- Aligné sur la politique d'IA, les valeurs et l'engagement responsable de l'entreprise
- Mesurable : indicateurs, résultats, réalisations concrètes
- Documenté et communiqué : consigné dans le système de management et diffusé aux équipes concernées
- Décliné au bon niveau pour une cohérence globale

Exemples d'objectifs d'IA concrets

- Développement responsable : Garantir que 100% des modèles IA sont revus humainement avant déploiement
- Performance et fiabilité : Atteindre au moins 95% de précision pour les modèles en production
- Transparence : Fournir à chaque utilisateur une explication claire des résultats produits par l'IA
- Éthique : Vérifier l'absence de biais de genre ou d'origine dans les jeux de données sensibles

Points clés à retenir

- Un objectif = un résultat concret et mesurable à atteindre
- Un objectif d'IA est spécifique au développement ou à l'usage de l'IA, et aligne la gouvernance sur la politique d'entreprise
- Des objectifs définis à tous les niveaux assurent la cohérence du système, le suivi de la performance, et la démonstration d'une maîtrise responsable de l'IA

Fiche pratique - Guide de rédaction de politique IA

Comment rédiger une politique IA ? (cf B.2.2 - AI policy)

Voici un guide pour rédiger une politique IA. Attention, cette politique sur l'IA n'a pas pour objectif d'être trop longue, mais plutôt de marquer les esprits.

Voici les différents paragraphes à prévoir dans votre politique :

Paragraphe	Activités
Mission	Expliquer les missions de l'organisme et comment l'IA s'intègre aux missions de l'organisme
Vision	Quelle est notre vision de l'IA et de la façon dont elle va être intégrée dans l'entreprise.
Contexte	• Contexte et périmètre d'application de la politique • Quels sont les produits, services concernés ? • Pourquoi ?
Indication et explication des objectifs d'IA	• Identifier les objectifs d'IA retenus et comment vous souhaitez les mettre en place. • Répondre à la question : qu'est-ce que je veux obtenir ? • Expliquer comment ceux-ci sont établis et revus
Responsabilités	Désigner les rôles responsables pour être responsable du SMIA et pour le reporting du SMIA à la Direction
Mentions obligatoires	• Engagement à mettre en place et améliorer un SMIA • Engagement à satisfaire aux obligations légales et règlementaires
Lien avec les autres politiques	Il est essentiel d'assurer la cohérence entre les différentes politiques en lien avec l'intelligence artificielle et les données. Parmi ces politiques clés, on retrouve notamment : • La politique Data & IA • La politique d'usage responsable • La politique d'évaluation d'impact • La politique tiers/fournisseurs • La politique de protection de la vie privée

Fiche pratique - Choisir ses contrôles
Les annexes A et B

Application des contrôles dans l'ISO 42001

La norme ISO 42001 n'impose pas de liste fixe de contrôles : elle exige que chaque organisation sélectionne et adapte les contrôles en fonction de son contexte et des risques liés à ses usages de l'IA. Ce choix s'effectue dans le cadre du système de management de l'IA (AIMS), suivant un processus structuré :

- Lors de l'analyse des risques, l'organisation identifie les menaces et opportunités propres aux systèmes d'IA, puis définit les politiques, actions et processus à mettre en œuvre pour les traiter.
- La sélection des contrôles peut s'appuyer sur des standards spécialisés : NIST, ANSI, CNIL, OWASP, ou d'autres référentiels sectoriels reconnus.
- Après sélection, il est essentiel de vérifier que les risques recensés sont bien couverts : cela se fait en analysant la conformité avec les contrôles de l'annexe A.

En résumé : le choix des contrôles dépend directement de l'analyse des risques IA réalisée sur les cas d'usage définis dans le périmètre du projet.

Rôle et utilisation de l'annexe A (ISO 42001:2023)

L'annexe A est une ressource informative : elle propose une liste thématique de contrôles recommandés pour aider à traiter les risques identifiés dans la démarche AIMS. Elle couvre des domaines majeurs tels que :

- Supervision humaine : garantir une supervision appropriée des systèmes IA
- Transparence et explicabilité : assurer la compréhension et l'explication des décisions IA
- Robustesse et sécurité : renforcer la fiabilité et la sécurité des modèles
- Qualité des données : veiller à la pertinence et à la fiabilité des données utilisées
- Gestion du cycle de vie : organiser les étapes clés du développement et de l'exploitation IA
- Engagement des parties prenantes : impliquer les acteurs concernés dans la gouvernance IA

Pour chaque domaine, des contrôles sont suggérés : ils peuvent être sélectionnés, adaptés ou complétés selon les besoins et le contexte organisationnel.

Exigences et meilleures pratiques

L'organisation doit pouvoir démontrer :

- Que les contrôles choisis répondent précisément aux risques identifiés (voir § 6.1.2 et § 6.1.3)
- Que la mise en œuvre des contrôles est documentée, vérifiable et maintenue dans le temps (cf. chapitres 8 à 10)

Bonnes pratiques :

- Ne pas appliquer l'annexe A « à la lettre » : chaque contrôle doit être explicitement lié à un risque identifié (approche par les risques).
- Utiliser l'annexe comme référentiel d'inspiration ou checklist pour s'assurer que les thématiques critiques sont bien couvertes.
- Produire systématiquement une matrice (déclaration d'applicabilité) expliquant la relation entre chaque risque et les contrôles associés, outil indispensable lors des audits.

Utilisation de l'annexe B

L'annexe B apporte un complément détaillé : elle fournit des exemples et des explications sur la mise en œuvre des contrôles thématiques, pour soutenir la conformité avec les exigences principales de la norme. Bien qu'elle ne soit pas obligatoire, elle est utile pour structurer la documentation et garantir le traitement cohérent des risques dans les domaines majeurs.

CONCLUSION

Nos services

06

Pourquoi FeelAgile ?

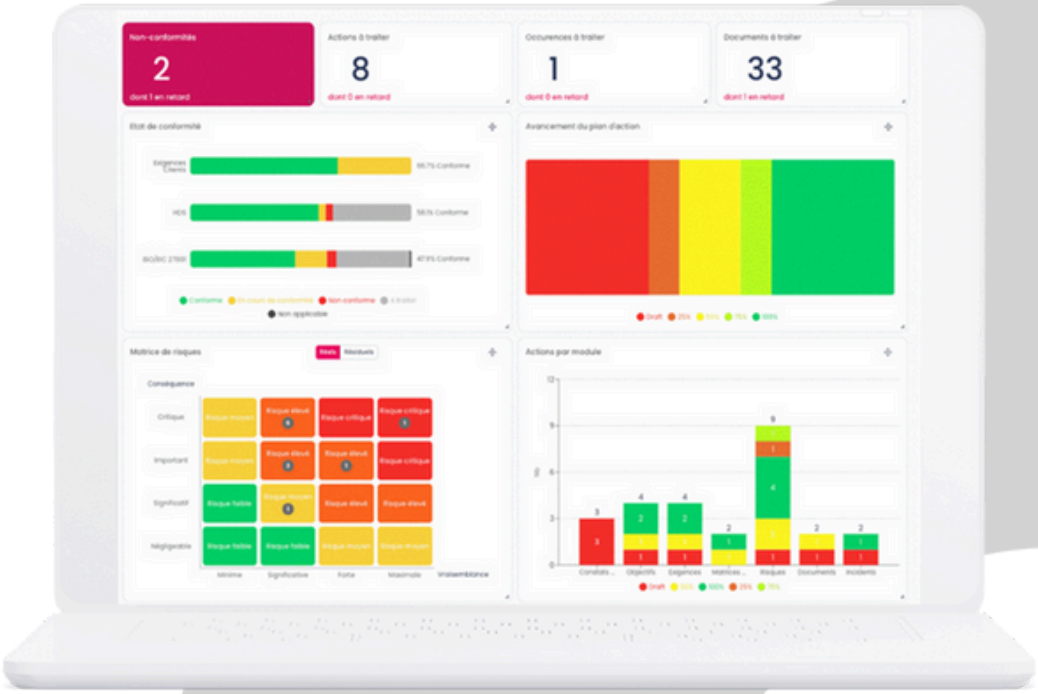
Anticipez l'avenir de l'ISO 42001 avec FeelAgile : une expertise certifiée, des outils agiles, et des résultats garantis. FeelAgile est le leader des certifications ISO en France avec plus de 200 entreprises certifiées et accompagnées.

- Une garantie d'être certifié à 100%
- Une combinaison d'expertises cybersécurité, juridique et organisationnelle
- Des solutions d'automatisation
- Une équipe support
- Des financements
- Une approche agile des certifications, sur mesure

Plateforme Oversecur : Votre atout ISO 42001

Centralisez, sécurisez et pilotez votre conformité ISO 42001 en toute simplicité.

- **Intégrez** toutes les **données** de votre démarche de **certification**
- **Centralisez l'information,** le suivi de vos actions et les **preuves** nécessaires pour l'audit
- Utilisez une **plateforme sécurisée** sur votre cloud ou en hébergement



- Multi-référentiels
- Automatisation des relances
- Gestion des risques
- Système documentaire intégré
- Outil sécurisé & collaboratif

OVERSECUR By FeelAgile

FeelAgile

Leader de l'ISO 27001

Votre partenaire expert pour une conformité agile et durable

EXPERTISE EN CERTIFICATION

20 ans

PASSÉS DANS LES ORGANISATIONS

16 Experts cyber, chefs de projet 27001, auditeurs

+ de 200 projets 27001

FeelAgile

Des services externalisés pour vos certifications ou votre conformité

FeelAgile OVERSECUR

Une plateforme SaaS pour vos certifications

FeelAgile LEARNING

Sensibilisations et formations pour vos collaborateurs

Certifié et reconnu par les meilleurs acteurs

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION

PECB AUTHORIZED PARTNER

numeum

CAMPUS CYBER

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

FeelAgile

Restons en contact !

Alexis Schuhmacher, Directeur Commercial

+33 6 34 42 67 08

aschuhmacher@feelagile.com

@alexisschuhmacher

https://feelagile.com/

Prendre rendez-vous

FeelAgile est le **leader des certifications** ISO 27001 en France avec **plus de 200 entreprises certifiées** et accompagnées.