AYI NEDJIMI Consultants

# ISO/IEC 42001 Foundation : Système de Management IA

Catégorie : Conformité  Lecture : 29 min  Publié le : 14/02/2026  Auteur : Ayi NEDJIMI

*Guide exhaustif ISO/IEC 42001 : première norme SMIA, architecture PDCA clauses 4-10, annexes A et B, contrôles IA, certification PECB Foundation.*

## Table des Matieres



Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

## 1 Qu'est-ce que l'ISO/IEC 42001 ?

Publiée le **18 décembre 2023** par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC), la norme **ISO/IEC 42001:2023** constitue une avancée historique dans le domaine de la gouvernance technologique. Elle est la **première norme internationale certifiable** spécifiquement dédiée à l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un **Système de Management de l'Intelligence Artificielle (SMIA)**. Cette norme répond à un besoin critique : alors que l'adoption de l'IA s'accélère dans tous les secteurs — santé, finance, industrie, administration publique —, les organisations manquaient jusqu'alors d'un cadre de référence structuré et universellement reconnu pour gérer de manière responsable et systématique leurs activités liées à l'intelligence artificielle.

## Contexte historique et genèse de la norme

L'histoire de l'ISO/IEC 42001 s'inscrit dans un mouvement global de régulation de l'intelligence artificielle qui a pris de l'ampleur à partir de 2018. Le **sous-comité ISO/IEC JTC 1/SC 42** (Intelligence artificielle), créé en octobre 2017, a été mandaté pour développer un ensemble de normes couvrant les différentes facettes de l'IA : terminologie (ISO/IEC 22989), concepts de gouvernance (ISO/IEC 38507), gestion des risques (ISO/IEC 23894), et système de management (ISO/IEC 42001). Le développement de la norme a mobilisé plus de **50 pays participants** et des centaines d'experts issus du monde académique, de l'industrie technologique, des organismes de régulation et de la société civile. Le processus normatif, étalé sur quatre années de travaux (2019-2023), a traversé les étapes classiques de l'ISO : proposition (NP), préparation (WD), comité (CD), enquête (DIS) et approbation (FDIS), avant la publication finale en décembre 2023.

**Notre avis d'expert**

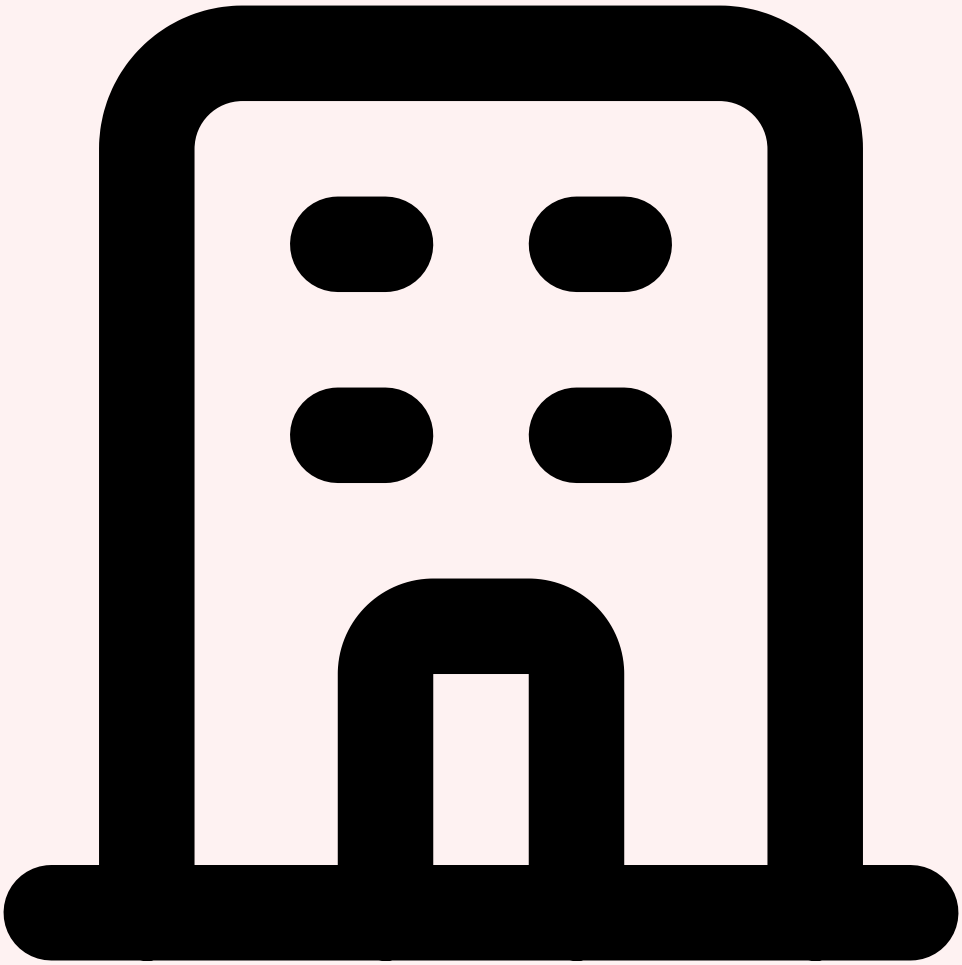
La conformité et la sécurité ne sont pas synonymes, mais elles sont complémentaires. L'ISO 27001 offre un cadre structurant qui, bien implémenté, améliore réellement la posture de sécurité. Le ROI d'une certification va bien au-delà du simple badge de conformité.

Ce calendrier n'est pas anodin : la publication de l'ISO/IEC 42001 est intervenue moins de deux semaines avant l'accord politique sur le **Règlement européen sur l'IA (AI Act)**, conclu le 8 décembre 2023 par le Parlement européen et le Conseil. Cette quasi-simultanéité n'est pas une coïncidence, mais le résultat d'une convergence stratégique entre les normalisateurs internationaux et les régulateurs européens. L'article 40 de l'AI Act prévoit explicitement que les **normes harmonisées** — dont l'ISO/IEC 42001 est la candidate naturelle — peuvent servir de présomption de conformité pour les systèmes d'IA à haut risque, créant ainsi un pont direct entre normalisation volontaire et régulation contraignante.

## Pourquoi un système de management spécifique à l'IA ?

La question est légitime : pourquoi ne pas simplement étendre l'ISO 27001 (sécurité de l'information) ou l'ISO 9001 (qualité) pour couvrir l'IA ? La réponse réside dans les **caractéristiques distinctives de l'IA** qui nécessitent des contrôles dédiés. Premièrement, les systèmes d'IA présentent un **comportement émergent** : contrairement aux systèmes déterministes classiques, un modèle de machine learning peut produire des résultats inattendus, y compris sur des données proches de celles de l'entraînement. Deuxièmement, la **dépendance aux données** est fondamentale : la qualité, la représentativité et la gouvernance des jeux de données d'entraînement et de test déterminent directement la performance et l'équité du système. Troisièmement, les **enjeux éthiques et sociétaux** sont spécifiques : biais algorithmiques, explicabilité des décisions, impact sur l'emploi, surveillance de masse, deepfakes. Quatrièmement, le **cycle de vie de l'IA** diffère fondamentalement du cycle de vie logiciel classique : entraînement, validation, déploiement, monitoring en production, réentraînement, décommissionnement, chaque étape introduisant des risques spécifiques qui ne sont pas couverts par les normes existantes.

**Point clé : Différences fondamentales ISO 42001 vs ISO 27001**
L'ISO 27001 protège la **confidentialité, l'intégrité et la disponibilité** de l'information. L'ISO 42001, tout en intégrant ces dimensions, ajoute des exigences spécifiques sur la **responsabilité algorithmique**, la **transparence des systèmes d'IA**, l'**équité et la non-discrimination**, la **robustesse et la fiabilité** des modèles, ainsi que l'**impact sociétal** de l'IA. Les deux normes sont complémentaires et conçues pour être intégrées grâce à la structure harmonisée (HLS).



## Champ d'application et applicabilité

L'ISO/IEC 42001 est volontairement **agnostique en termes de taille d'organisation et de secteur d'activité**. Elle s'adresse aussi bien à une startup développant un chatbot qu'à un groupe industriel déployant des systèmes de vision par ordinateur sur ses lignes de production. Le périmètre du SMIA est défini par l'organisation elle-même, conformément à la clause 4.3, et peut couvrir l'ensemble des activités IA ou se limiter à un département, un produit ou un cas d'usage spécifique. La norme s'applique aux organisations qui **développent, fournissent ou utilisent** des systèmes d'IA, reconnaissant ainsi la diversité

des rôles dans l'écosystème IA. Un éditeur de logiciel IA, un intégrateur, un opérateur cloud proposant des services d'IA, ou une entreprise utilisatrice qui intègre des API d'IA tierces : tous peuvent se certifier ISO 42001, chacun adaptant le périmètre et les contrôles à son contexte spécifique.

En février 2026, **plus de 200 organisations** ont déjà obtenu la certification ISO/IEC 42001 dans le monde, un rythme d'adoption remarquablement rapide comparé aux premiers mois de l'ISO 27001 en 2005. Les secteurs en pointe incluent les services financiers, la santé numérique, les télécommunications et les éditeurs de solutions IA. En France, l'AFNOR a accrédité plusieurs organismes de certification pour l'ISO 42001, et le **COFRAC** supervise la compétence des auditeurs. L'ANSSI, bien que n'étant pas directement impliquée dans la certification ISO 42001, reconnaît la norme comme un élément structurant de la **confiance numérique** dans le cadre de la stratégie nationale pour l'IA.

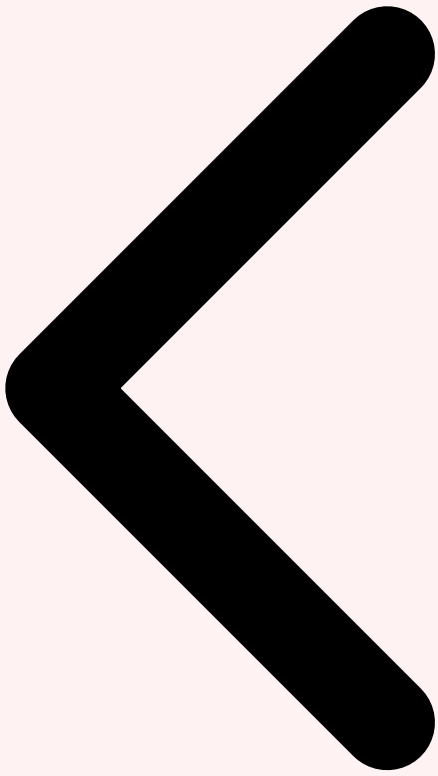
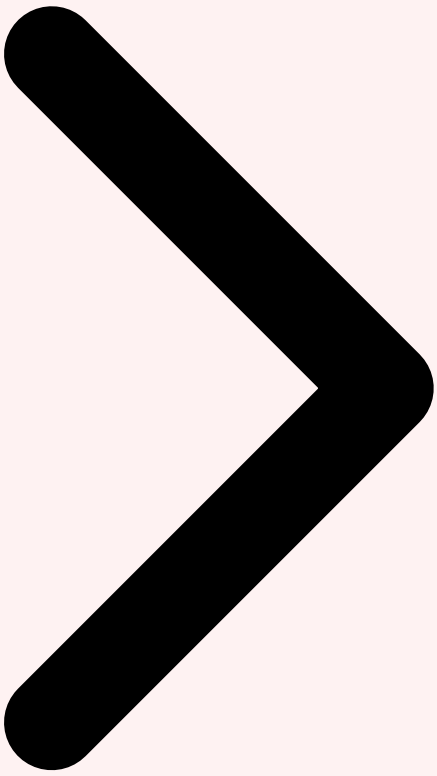


Table des Matieres Qu'est-ce que l'ISO/IEC 42001 ? Architecture de la Norme



**Cas concret**
L'amende record de 150 millions d'euros infligée par la CNIL à Google en 2022 pour non-conformité aux règles de gestion des cookies a envoyé un signal fort à l'industrie. Cette décision a accéléré l'adoption des Consent Management Platforms et la révision des pratiques de tracking publicitaire en Europe.

Êtes-vous certain que votre traitement des données personnelles est conforme au RGPD ?

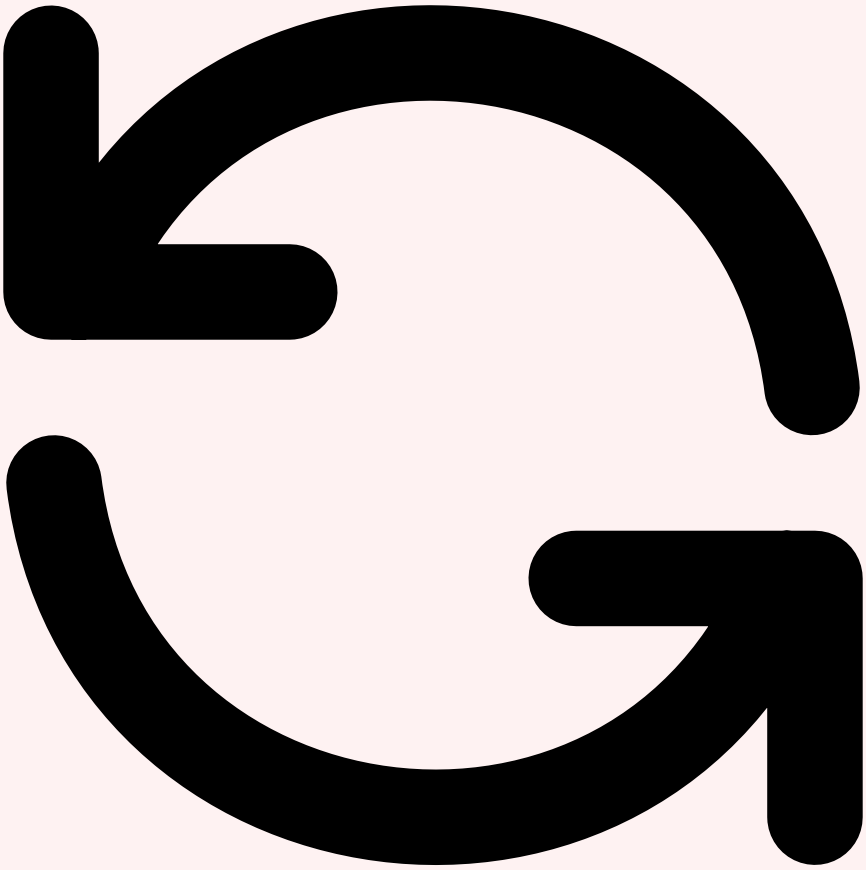
## 2 Architecture de la Norme : Structure Harmonisée et PDCA

L'ISO/IEC 42001 adopte la **Structure Harmonisée de Haut Niveau (HLS — Harmonized Structure)** définie dans l'Annexe SL des Directives ISO/IEC, Partie 1. Cette structure, commune à toutes les normes de systèmes de management modernes (ISO 27001, ISO 9001, ISO 14001, ISO 22301, etc.), garantit la compatibilité et l'intégrabilité entre les différents systèmes de management d'une organisation. Pour les entreprises déjà certifiées ISO 27001, cette architecture familière facilite considérablement l'extension du système de management existant pour intégrer les exigences spécifiques à l'IA.

### Les 10 clauses de la HLS

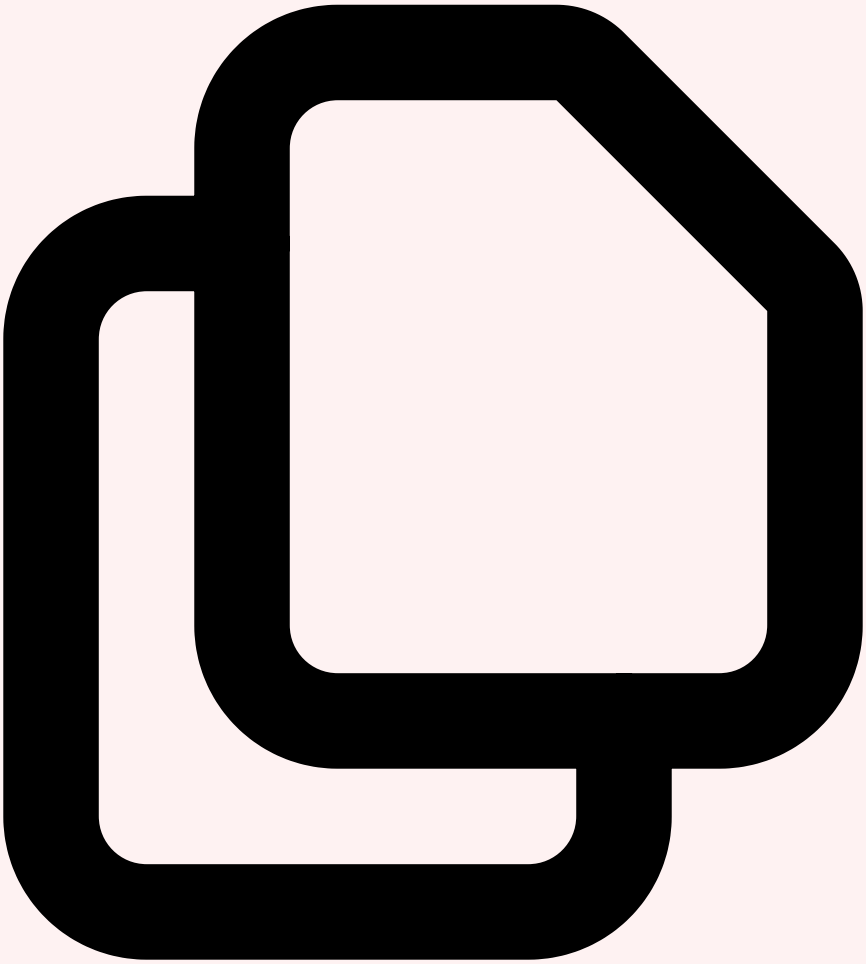
La norme est structurée en **10 clauses principales**, dont les clauses 1 à 3 sont introductives (domaine d'application, références normatives, termes et définitions) et les clauses 4 à 10 contiennent les exigences normatives auditables. L'architecture HLS impose un vocabulaire commun, des exigences fondamentales identiques et une logique de cycle d'amélioration continue PDCA (Plan-Do-Check-Act) qui structure l'ensemble du système de management.

| Clause | Titre | Phase PDCA | Objectif principal |
|---|---|---|---|
| 4 | Contexte de l'organisation | Plan | Comprendre l'environnement et le périmètre du SMIA |
| 5 | Leadership | Plan | Engagement de la direction et politique IA |
| 6 | Planification | Plan | Traiter les risques et définir les objectifs IA |
| 7 | Support | Plan | Fournir les ressources et compétences nécessaires |
| 8 | Fonctionnement | Do | Mettre en œuvre les processus et contrôles IA |
| 9 | Évaluation des performances | Check | Surveiller, mesurer et auditer le SMIA |
| 10 | Amélioration | Act | Corriger les écarts et améliorer en continu |



### Le cycle PDCA appliqué à l'IA

Le cycle **Plan-Do-Check-Act (PDCA)**, hérité des travaux de Deming et Shewhart, constitue le moteur de l'amélioration continue du SMIA. Dans le contexte spécifique de l'IA, chaque phase du cycle acquiert une signification particulière. La phase **Plan** (clauses 4-7) comprend l'analyse du contexte organisationnel vis-à-vis de l'IA, l'engagement de la direction dans une politique IA explicite, l'identification et le traitement des risques spécifiques aux systèmes d'IA, et la mobilisation des ressources humaines et techniques nécessaires. La phase **Do** (clause 8) couvre la mise en œuvre opérationnelle : développement, déploiement et exploitation des systèmes d'IA conformément aux plans établis, incluant l'appréciation et le traitement des risques IA, ainsi que l'analyse d'impact. La phase **Check** (clause 9) organise la surveillance des performances du SMIA et des systèmes d'IA en production, les audits internes et la revue de direction. Enfin, la phase **Act** (clause 10) traite les non-conformités détectées et pilote l'amélioration continue du système.

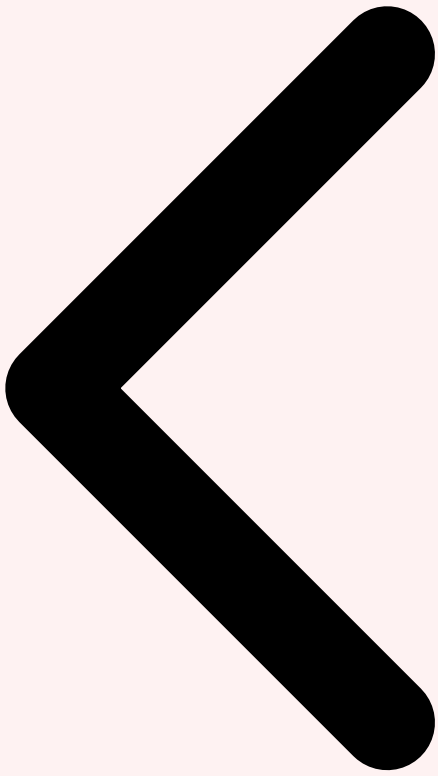


### Spécificités par rapport aux autres normes HLS

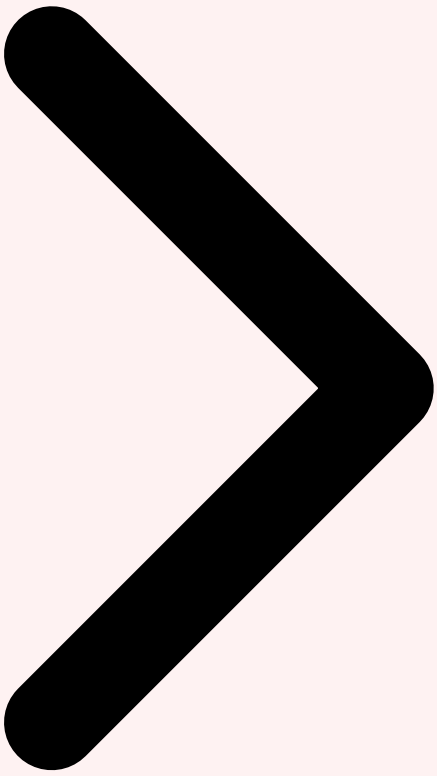
Bien que l'ISO/IEC 42001 partage la même structure que l'ISO 27001, elle introduit des **exigences spécifiques absentes des autres normes HLS**. La clause 8.4, par exemple, est entièrement dédiée à l'**analyse d'impact des systèmes d'IA**, une exigence sans équivalent dans l'ISO 27001. De même, la clause 6.1.2 sur l'appréciation des risques IA impose de considérer des catégories de risques propres à l'IA : biais algorithmiques, dérive des modèles (model drift), attaques adversariales, défaillances en conditions hors distribution, impacts sur les droits fondamentaux. Les annexes A et B, que nous détaillerons dans la section 5, constituent également un apport majeur : là où l'ISO 27001 propose 93 contrôles de sécurité de l'information dans son Annexe A, l'ISO 42001 propose un ensemble de **contrôles spécifiquement conçus pour la gouvernance de l'IA**, couvrant des domaines comme la transparence algorithmique, l'explicabilité, la qualité des données d'entraînement, et la supervision humaine des décisions automatisées. Pour approfondir, consultez Aspects Juridiques et Éthiques de l'IA : Cadre Réglementaire.

**Attention : Intégration ne signifie pas substitution**

L'ISO/IEC 42001 ne remplace pas l'ISO 27001. Une organisation développant des systèmes d'IA traitant des données personnelles ou sensibles aura besoin des **deux certifications** : l'ISO 27001 pour la sécurité de l'information et l'ISO 42001 pour la gouvernance de l'IA. La HLS facilite leur intégration dans un système de management unique, mais chaque norme couvre des exigences distinctes et complémentaires.

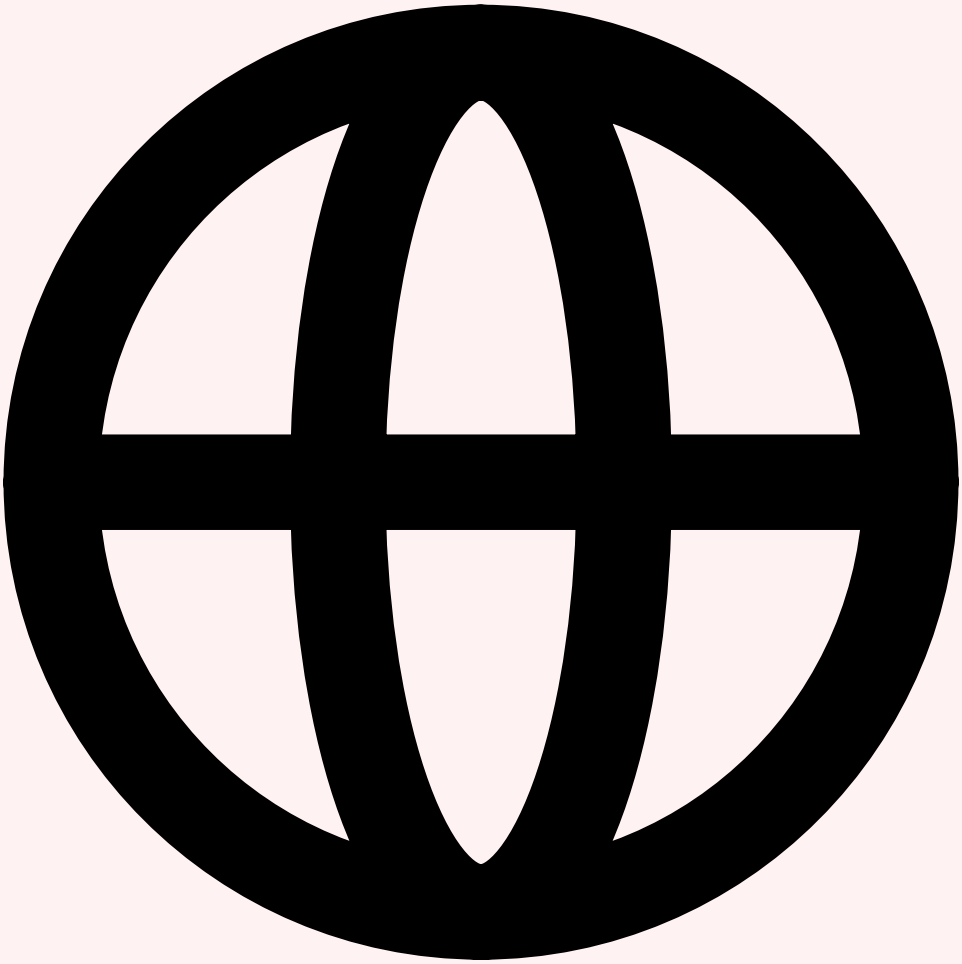


Qu'est-ce que l'ISO/IEC 42001 ? Architecture de la Norme Exigences Fondamentales (4-7)



## 3 Exigences Fondamentales : Clauses 4 à 7

Les clauses 4 à 7 constituent le socle du SMIA. Elles définissent le **cadre stratégique, organisationnel et de support** sur lequel repose l'ensemble du système de management. Ces clauses correspondent à la phase « Plan » du cycle PDCA et déterminent la capacité de l'organisation à concevoir, déployer et maintenir un système d'IA responsable et conforme. Examinons chacune de ces clauses en détail, avec leurs implications pratiques pour les organisations.

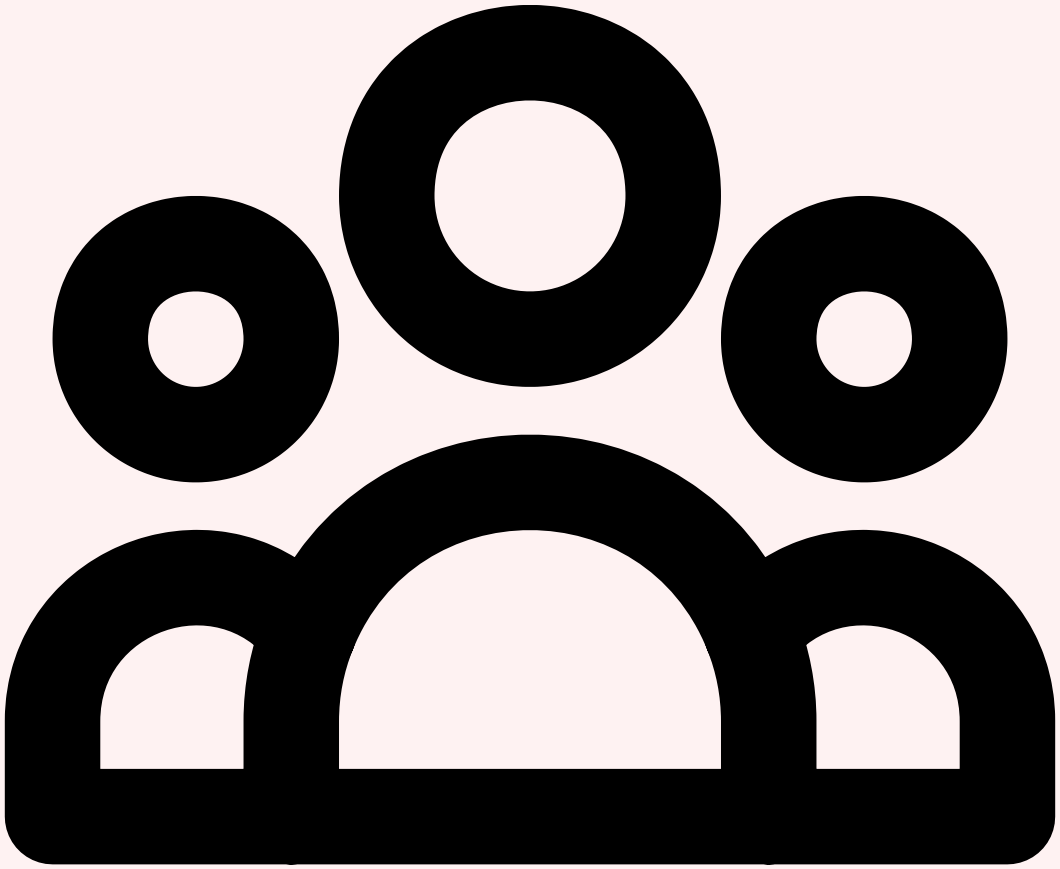


### Clause 4 : Contexte de l'organisation

La clause 4 impose à l'organisation de **comprendre son environnement** dans le contexte spécifique de l'IA. La sous-clause 4.1 exige l'identification des enjeux internes et externes pertinents : technologies d'IA utilisées ou envisagées, maturité de l'organisation en matière d'IA, cadre réglementaire applicable (AI Act, RGPD, réglementations sectorielles), attentes sociétales en matière d'IA responsable, état de l'art technologique et ses évolutions prévisibles. La sous-clause 4.2 requiert l'identification des **parties intéressées** et de leurs exigences : régulateurs (CNIL, autorités de marché), clients et utilisateurs des systèmes d'IA, personnes affectées par les décisions automatisées, employés, fournisseurs de technologies IA, organismes de normalisation, et société civile. Cette cartographie des parties intéressées est fondamentale car elle conditionne l'ensemble des contrôles à mettre en place.

La sous-clause 4.3, **détermination du domaine d'application**, est stratégiquement cruciale. L'organisation doit définir les limites et l'applicabilité du SMIA en tenant compte des enjeux identifiés en 4.1 et des exigences des parties intéressées en 4.2. Le périmètre peut couvrir l'ensemble des activités IA de l'organisation ou se limiter à certains systèmes, départements ou cas d'usage. La clause 4.4 exige ensuite que l'organisation établisse,

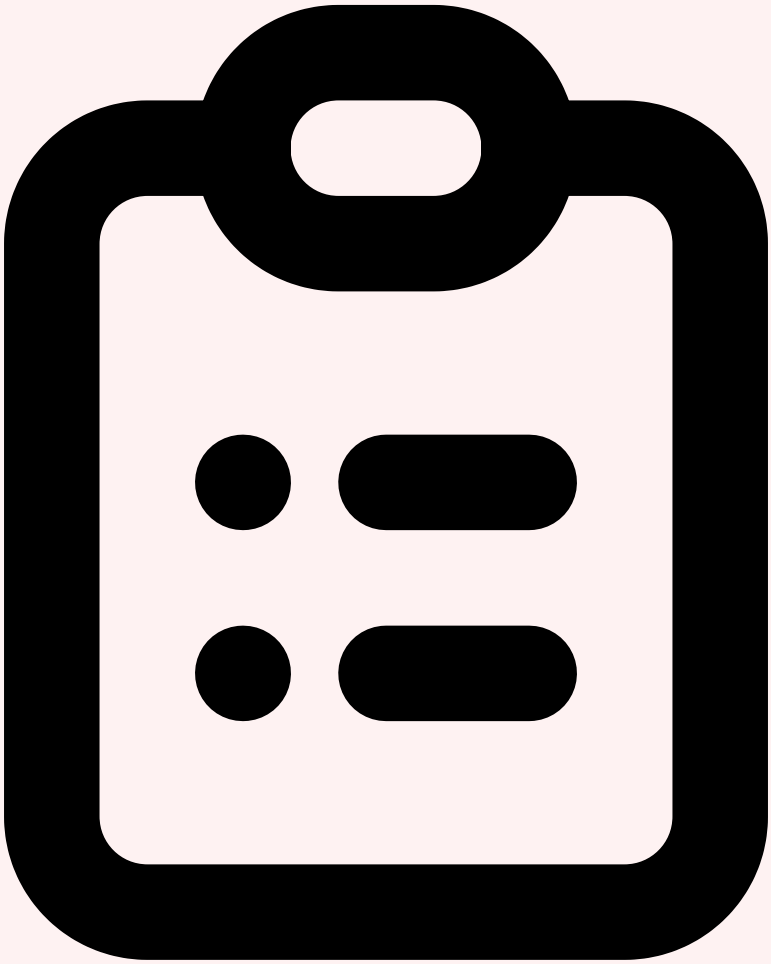
mette en œuvre, maintienne et améliore en continu le SMIA, incluant les processus nécessaires et leurs interactions, conformément aux exigences de la norme. Un élément distinctif de l'ISO 42001 par rapport à l'ISO 27001 est l'exigence explicite de prendre en compte le **cycle de vie complet des systèmes d'IA** dans la définition du périmètre, depuis la conception et le développement jusqu'au retrait et à la désactivation.



### Clause 5 : Leadership

La clause 5 place la **direction au cœur du SMIA**. La sous-clause 5.1 exige que la direction démontre son leadership et son engagement envers le SMIA par des actions concrètes : s'assurer que la politique et les objectifs IA sont établis et compatibles avec l'orientation stratégique de l'organisation, intégrer les exigences du SMIA dans les processus métiers, mettre à disposition les ressources nécessaires, communiquer sur l'importance d'un management efficace de l'IA et de la conformité aux exigences du SMIA, s'assurer que le SMIA atteint ses résultats prévus, et diriger et soutenir les personnes contribuant à l'efficacité du SMIA.

La sous-clause 5.2 impose l'établissement d'une **politique IA formelle**. Cette politique doit être appropriée à la finalité de l'organisation, fournir un cadre pour la définition des objectifs IA, inclure un engagement à satisfaire les exigences applicables (réglementaires, contractuelles, éthiques), et inclure un engagement d'amélioration continue du SMIA. La politique IA doit explicitement aborder l'**utilisation responsable de l'IA**, les principes éthiques auxquels l'organisation adhère, la gouvernance des données d'entraînement, la transparence envers les parties prenantes, et les mécanismes de supervision humaine. Elle doit être disponible sous forme d'information documentée, communiquée au sein de l'organisation et accessible aux parties intéressées pertinentes.

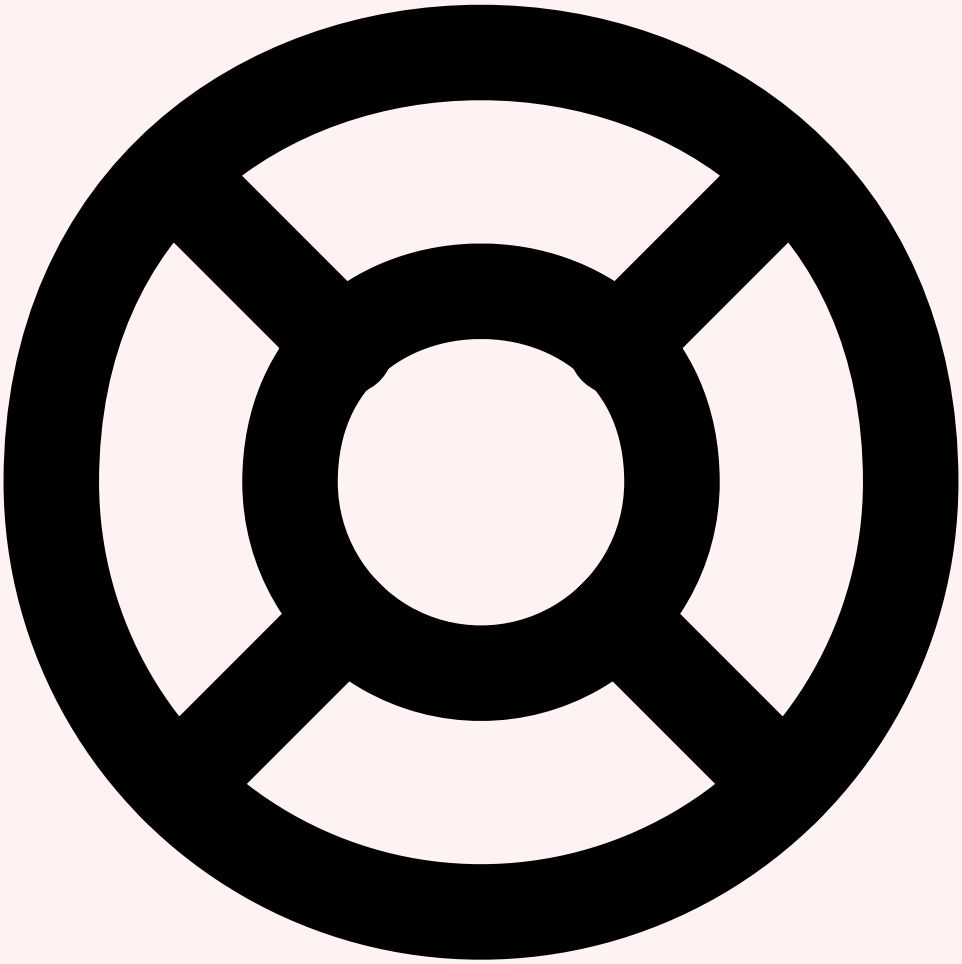


## Clause 6 : Planification

La clause 6 est le cœur analytique de la phase Plan. La sous-clause 6.1.1 exige que l'organisation prenne en compte les enjeux (4.1) et les exigences (4.2) pour déterminer les **risques et opportunités** qui nécessitent d'être traités pour donner l'assurance que le SMIA peut atteindre ses résultats, prévenir ou réduire les effets indésirables, et atteindre l'amélioration continue. La sous-clause 6.1.2, spécifique à l'IA, impose un processus

d'**appréciation des risques IA** qui doit établir et maintenir des critères de risque IA (incluant les critères d'acceptation), s'assurer que les appréciations répétées produisent des résultats cohérents, et identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité des informations dans le contexte du SMIA, mais aussi les risques de biais, d'inexplicabilité, de non-robustesse et d'impact sur les droits fondamentaux.

La sous-clause 6.1.3 concerne le **traitement des risques IA**. L'organisation doit sélectionner les options de traitement appropriées (éviter, transférer, réduire, accepter), déterminer les contrôles nécessaires en se référant à l'Annexe A, produire une **Déclaration d'Applicabilité (SoA)** documentant les contrôles sélectionnés et les justifications d'inclusion ou d'exclusion, et formuler un plan de traitement des risques IA. La sous-clause 6.2 exige l'établissement d'**objectifs IA mesurables** aux fonctions et niveaux pertinents, cohérents avec la politique IA, mesurables, tenant compte des exigences applicables, surveillés, communiqués et mis à jour si nécessaire.



### Clause 7 : Support

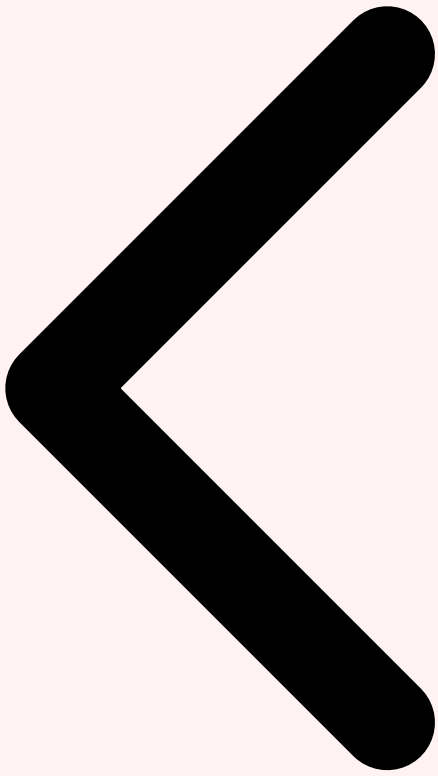
La clause 7 traite des **moyens nécessaires au fonctionnement du SMIA**. La sous-clause 7.1 (Ressources) exige la détermination et la mise à disposition des ressources nécessaires : budget, infrastructure technique (GPU, plateformes MLOps, outils de monitoring), et temps des collaborateurs. La sous-clause 7.2 (Compétences) impose que les personnes effectuant un travail ayant une incidence sur les performances du SMIA soient compétentes sur la base d'une formation initiale ou professionnelle, d'un savoir-faire et/ou d'une expérience appropriée. Dans le contexte de l'IA, cela implique des compétences en **data science, ingénierie ML, éthique de l'IA, gestion des risques IA** et compréhension réglementaire. L'organisation doit déterminer les compétences nécessaires, s'assurer que ces personnes sont compétentes, mener des actions pour acquérir les compétences manquantes et conserver des informations documentées comme preuves de compétence.

La sous-clause 7.3 (Sensibilisation) exige que les personnes effectuant un travail sous le contrôle de l'organisation soient sensibilisées à la politique IA, à leur contribution à l'efficacité du SMIA, et aux implications de la non-conformité aux exigences du SMIA. La sous-clause 7.4 (Communication) impose de déterminer les besoins en communication interne et externe relatifs au SMIA. Enfin, la sous-clause 7.5 (Informations documentées)

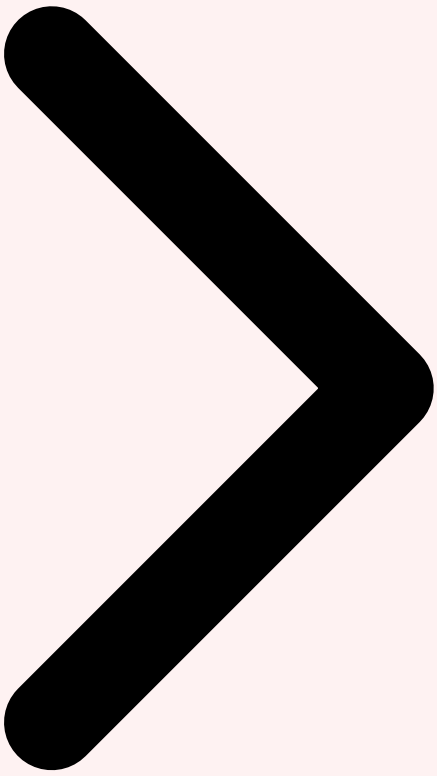
définit les exigences de **documentation du SMIA** : le SMIA doit inclure les informations documentées exigées par la norme et celles jugées nécessaires par l'organisation pour l'efficacité du SMIA, avec des procédures de création, mise à jour, maîtrise et conservation.

**Documentation minimale exigée par l'ISO/IEC 42001**

- ●**Politique IA** (5.2) — Document cadre approuvé par la direction
- ●**Périmètre du SMIA** (4.3) — Limites et applicabilité
- ●**Processus d'appréciation des risques IA** (6.1.2) — Méthodologie et critères
- ●**Plan de traitement des risques IA** (6.1.3) — Actions et responsabilités
- ●**Déclaration d'Applicabilité (SoA)** (6.1.3) — Contrôles Annexe A sélectionnés
- ●**Objectifs IA** (6.2) — Mesurables et suivis
- ●**Preuves de compétence** (7.2) — Formations, certifications, expérience
- ●**Résultats des appréciations de risques** (8.2) — Registre des risques IA
- ●**Résultats d'audit interne** (9.2) et **revue de direction** (9.3)

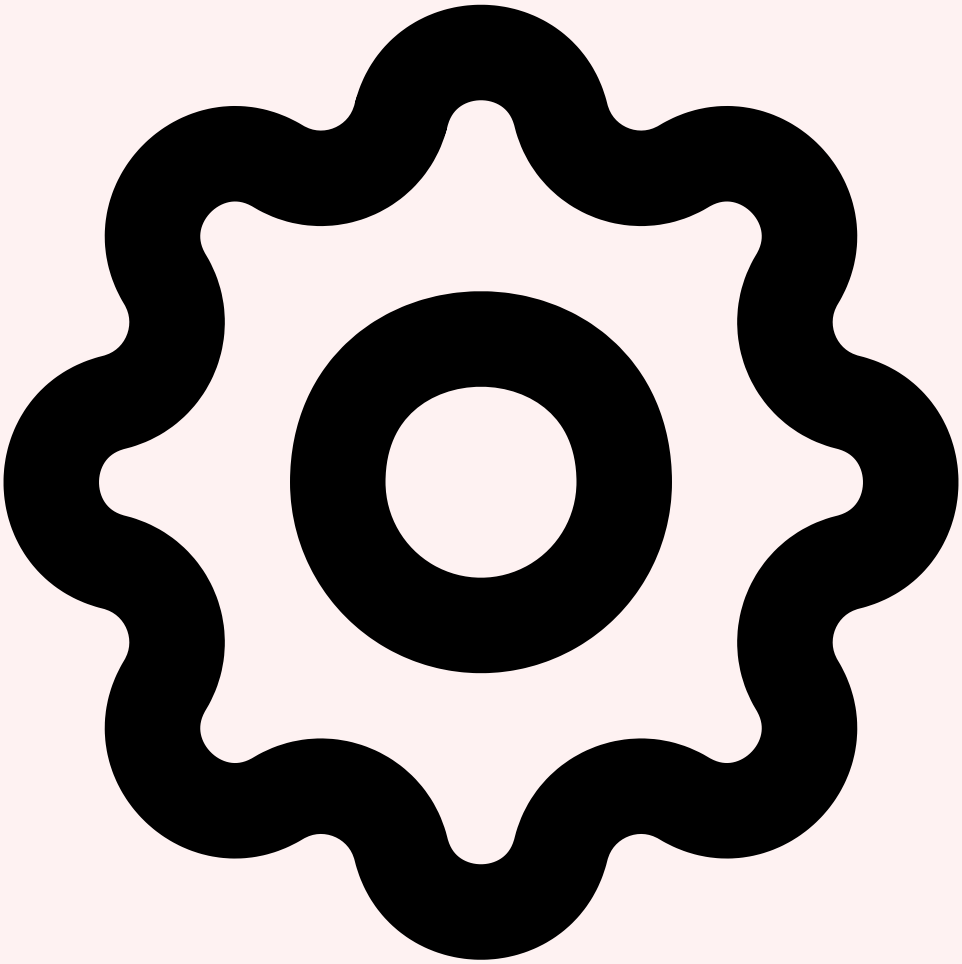


Architecture de la Norme Exigences Fondamentales (4-7) Exigences Opérationnelles (8-10)



## 4 Exigences Opérationnelles : Clauses 8 à 10

Les clauses 8 à 10 constituent le **cœur opérationnel du SMIA**, couvrant les phases Do, Check et Act du cycle PDCA. C'est dans ces clauses que la norme se distingue le plus des autres normes HLS, avec des exigences spécifiquement adaptées aux réalités opérationnelles des systèmes d'intelligence artificielle. Alors que les clauses 4 à 7 définissent le cadre et la planification, les clauses 8 à 10 prescrivent comment les organisations doivent concrètement exploiter, surveiller et améliorer leurs systèmes d'IA. Pour approfondir, consultez ISO 42001 Lead Implementer : Management de l'IA et Certification.



### Clause 8 : Fonctionnement

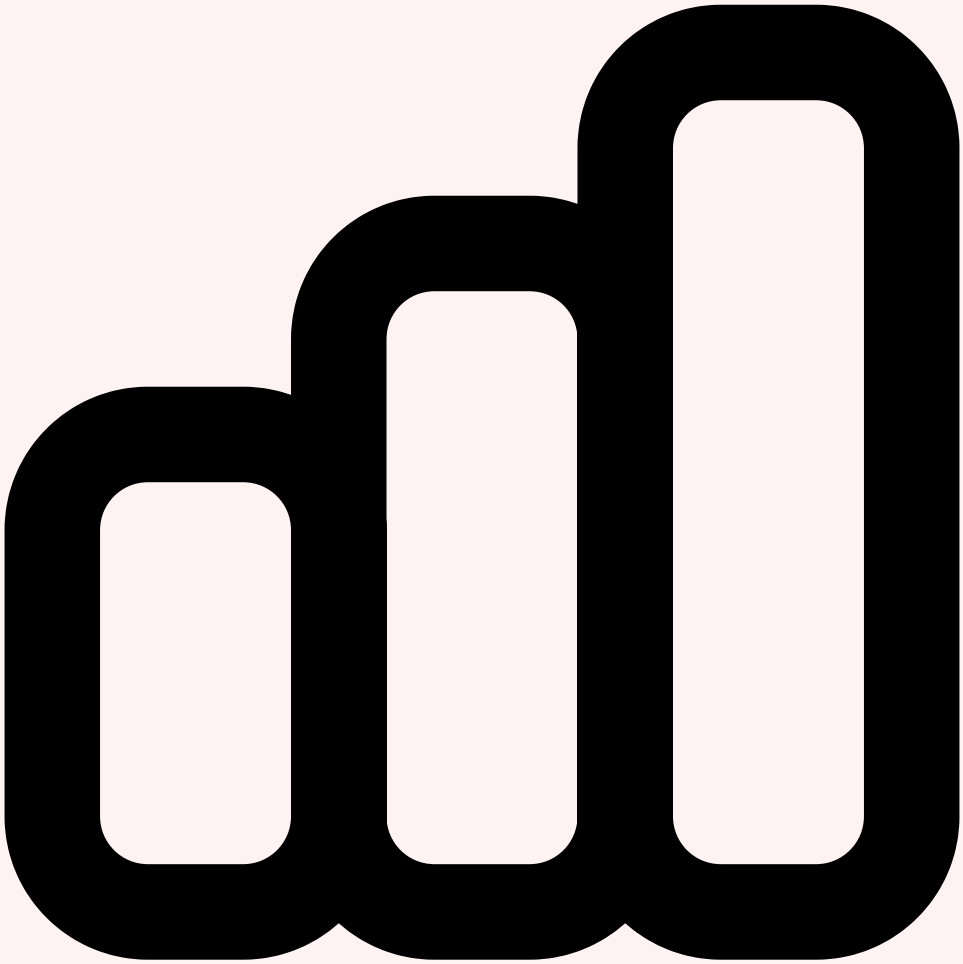
La clause 8 est la clause la plus substantielle de l'ISO/IEC 42001 et celle qui la distingue le plus fondamentalement des autres normes de systèmes de management. Elle comprend quatre sous-clauses majeures. La sous-clause **8.1 (Planification et maîtrise opérationnelles)** exige que l'organisation planifie, mette en œuvre et maîtrise les processus nécessaires pour satisfaire les exigences du SMIA et réaliser les actions déterminées en clause 6. Cela inclut l'établissement de critères pour les processus, la mise en œuvre de la maîtrise des processus conformément aux critères, et la conservation des informations documentées dans la mesure nécessaire pour avoir l'assurance que les processus ont été réalisés comme prévu. L'organisation doit maîtriser les modifications planifiées et analyser les conséquences des modifications imprévues, en menant des actions pour limiter tout effet négatif si nécessaire. Elle doit également s'assurer que les processus externalisés sont déterminés et maîtrisés.

La sous-clause **8.2 (Appréciation des risques IA)** exige que l'organisation réalise des appréciations des risques IA à des intervalles planifiés, ou lorsque des modifications significatives sont proposées ou se produisent, en tenant compte des critères établis en 6.1.2. Cette évaluation des risques doit couvrir l'ensemble du cycle de vie du système d'IA :

conception, développement, test, déploiement, exploitation, maintenance et retrait. Les risques spécifiques à évaluer incluent les **risques de biais et de discrimination** (le système traite-t-il équitablement tous les groupes de population ?), les **risques de robustesse** (comment le système se comporte-t-il face à des données adversariales ou hors distribution ?), les **risques d'explicabilité** (les décisions du système sont-elles interprétables par les utilisateurs et les personnes affectées ?), les **risques de dérive** (les performances du système se dégradent-elles dans le temps ?), et les **risques d'impact sur les droits fondamentaux**.

La sous-clause **8.3 (Traitement des risques IA)** exige la mise en œuvre du plan de traitement des risques IA défini en 6.1.3, incluant la sélection et l'implémentation des contrôles de l'Annexe A. L'organisation doit conserver les informations documentées sur les résultats du traitement des risques IA. La sous-clause **8.4 (Analyse d'impact du système d'IA)** est une innovation majeure de l'ISO 42001 sans équivalent dans l'ISO 27001. Elle exige que l'organisation réalise et documente une analyse d'impact pour chaque système d'IA relevant du périmètre du SMIA, évaluant les impacts potentiels sur les individus, les groupes de personnes et les sociétés. Cette analyse doit considérer les impacts directs et indirects, les impacts à court et long terme, et les impacts sur les droits fondamentaux et les libertés individuelles.

| Sous-clause 8.x | Exigence clé | Livrables documentés | Fréquence |
|---|---|---|---|
| 8.1 | Maîtrise opérationnelle | Procédures, critères de processus | Continue |
| 8.2 | Appréciation des risques IA | Registre des risques IA | Planifiée + changements |
| 8.3 | Traitement des risques IA | Plan de traitement, SoA mise à jour | Après chaque appréciation |
| 8.4 | Analyse d'impact système IA | Rapport d'impact par système IA | Par système + revue périodique |



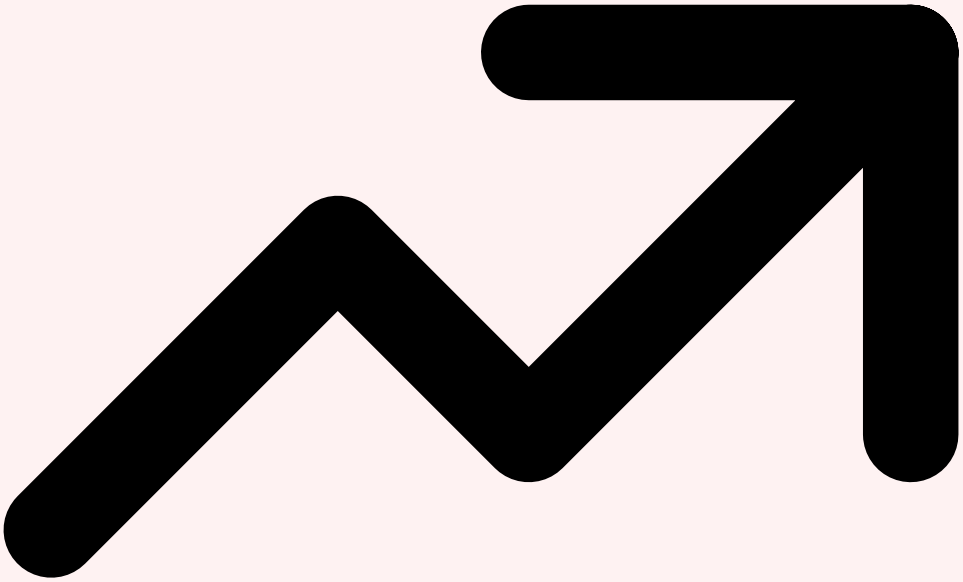
## Clause 9 : Évaluation des performances

La clause 9 structure la **phase Check du cycle PDCA**. La sous-clause 9.1 (Surveillance, mesure, analyse et évaluation) exige que l'organisation détermine ce qu'il est nécessaire de surveiller et mesurer (y compris les processus et les contrôles du SMIA), les méthodes de surveillance, mesure, analyse et évaluation, le moment où les activités de surveillance et de mesure doivent être effectuées, et le moment où les résultats de surveillance et de mesure doivent être analysés et évalués. Dans le contexte de l'IA, cela se traduit par la mise en œuvre d'**indicateurs de performance** couvrant à la fois le SMIA lui-même (taux de conformité aux contrôles, délais de traitement des non-conformités, maturité du système de management) et les systèmes d'IA individuels (performance prédictive, taux de dérive, équité entre groupes démographiques, taux d'utilisation, satisfaction des utilisateurs).

La sous-clause **9.2 (Audit interne)** exige la réalisation d'audits internes à des intervalles planifiés pour déterminer si le SMIA est conforme aux exigences propres de l'organisation et à celles de la norme ISO/IEC 42001, et s'il est efficacement mis en œuvre et maintenu. L'organisation doit planifier, établir, mettre en œuvre et maintenir un programme d'audit prenant en considération l'importance des processus concernés et les résultats des audits

précédents, définir les critères d'audit et le périmètre de chaque audit, sélectionner des auditeurs compétents et objectifs, et s'assurer que les résultats des audits sont rapportés à la direction concernée. Les compétences requises pour les auditeurs internes SMIA incluent la maîtrise de la norme ISO/IEC 42001, la compréhension des technologies d'IA auditées, et la connaissance des risques spécifiques à l'IA.

La sous-clause **9.3 (Revue de direction)** exige que la direction de l'organisation procède à la revue du SMIA à des intervalles planifiés, pour s'assurer de sa pertinence, de son adéquation et de son efficacité continues. Les éléments d'entrée de la revue de direction doivent inclure : l'état d'avancement des actions décidées lors des revues de direction précédentes, les modifications des enjeux internes et externes pertinents pour le SMIA, les retours d'information sur les performances du SMIA (y compris les tendances concernant les non-conformités et les actions correctives, les résultats de surveillance et de mesure, les résultats d'audit, et l'atteinte des objectifs IA), les retours d'information des parties intéressées, les résultats des appréciations des risques IA et l'état du plan de traitement des risques, et les opportunités d'amélioration continue.



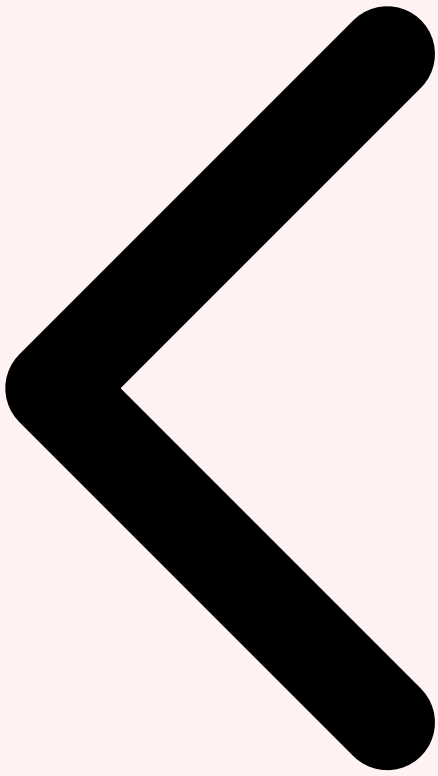
### Clause 10 : Amélioration

La clause 10 ferme la boucle PDCA avec la **phase Act**. La sous-clause 10.1 (Non-conformité et action corrective) exige que lorsqu'une non-conformité se produit, l'organisation réagisse en prenant des mesures pour la maîtriser et la corriger, en traitant les conséquences, en évaluant s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité (afin qu'elle ne se reproduise pas), en mettant en œuvre toute action requise, en passant en revue l'efficacité de toute action corrective mise en œuvre, et en modifiant le SMIA si nécessaire. Dans le contexte de l'IA, une non-conformité peut prendre des formes variées : un système d'IA produisant des résultats biaisés détectés lors d'un audit, une défaillance de monitoring entraînant une dérive non détectée, un manquement à l'obligation de transparence envers les utilisateurs, ou encore un incident de sécurité affectant les données d'entraînement.

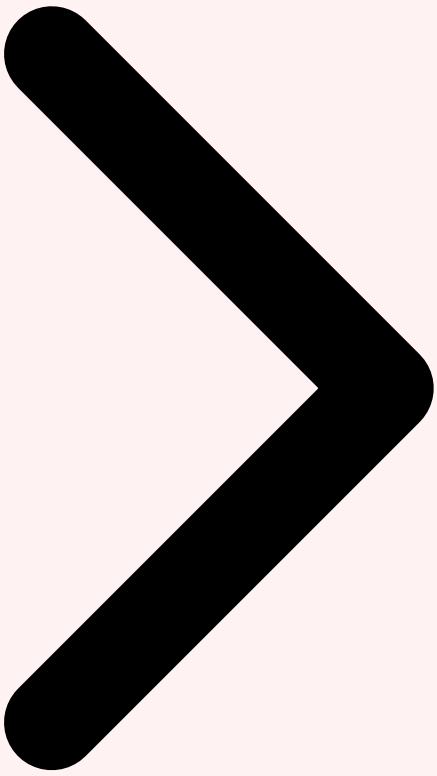
La sous-clause **10.2 (Amélioration continue)** exige que l'organisation améliore en continu la pertinence, l'adéquation et l'efficacité du SMIA. Cette exigence se traduit par une vigilance permanente sur l'évolution du contexte réglementaire (AI Act, RGPD, réglementations sectorielles), des technologies d'IA (nouveaux modèles, nouvelles vulnérabilités), des attentes des parties intéressées, et des bonnes pratiques sectorielles.

L'amélioration continue implique également le benchmark régulier avec les pratiques des pairs, la participation aux travaux de normalisation, et l'intégration des retours d'expérience des incidents et des audits dans l'évolution du SMIA.

**Exigence critique : Traçabilité des non-conformités IA**
Contrairement aux non-conformités classiques, les non-conformités IA peuvent avoir des **impacts différés et systémiques**. Un biais détecté dans un modèle de scoring de crédit, par exemple, a potentiellement affecté des milliers de décisions passées. La norme exige une analyse de l'étendue de l'impact, une remédiation des conséquences pour les personnes affectées, et des mesures préventives robustes. L'organisation doit conserver des informations documentées comme preuves de la nature des non-conformités et de toute action menée, ainsi que des résultats de toute action corrective.



Exigences Fondamentales (4-7) Exigences Opérationnelles (8-10) Annexes A et B



## 5 Annexes A et B : Contrôles et Objectifs de Mise en Œuvre

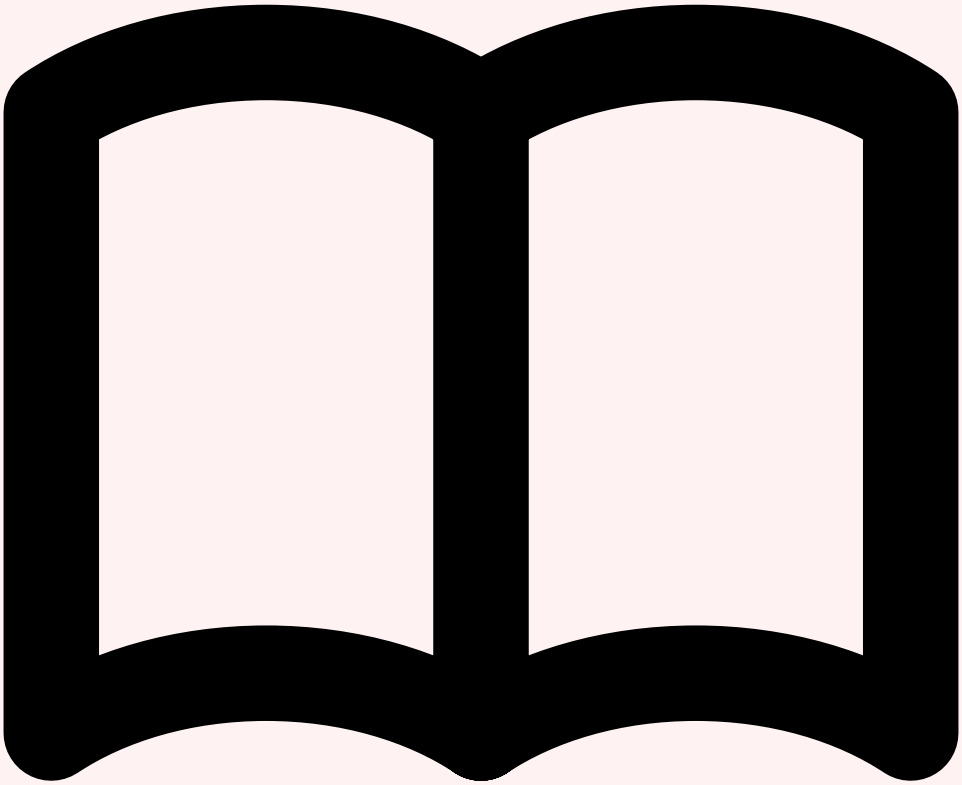
Les annexes de l'ISO/IEC 42001 constituent l'un des apports les plus concrets et opérationnels de la norme. Si les clauses 4 à 10 définissent le cadre du système de management, les annexes fournissent les **contrôles spécifiques et les objectifs de mise en œuvre** qui donnent corps au SMIA. L'Annexe A (normative) présente les contrôles de référence que l'organisation doit évaluer et, le cas échéant, mettre en œuvre. L'Annexe B (normative) détaille les objectifs de mise en œuvre associés à chaque contrôle. Les Annexes C et D (informatives) fournissent des orientations complémentaires sur les objectifs organisationnels liés à l'IA et l'utilisation des systèmes d'IA dans différents domaines.

### Annexe A : Les 39 contrôles de référence

L'Annexe A de l'ISO/IEC 42001 contient **39 contrôles** répartis en 9 domaines (A.2 à A.10). Chaque contrôle est identifié par un numéro et un titre, accompagné d'un attribut (type de contrôle) et d'une description de l'objectif de contrôle. Contrairement à l'ISO 27001 qui impose 93 contrôles de sécurité dans son Annexe A, l'ISO 42001 propose un ensemble plus resserré mais spécifiquement adapté aux enjeux de l'intelligence artificielle. L'organisation sélectionne les contrôles applicables à son contexte via la **Déclaration d'Applicabilité (SoA — Statement of Applicability)** et justifie l'exclusion de tout contrôle non retenu.

Le domaine **A.2 (Politiques relatives à l'IA)** couvre l'établissement de politiques IA formelles, incluant la politique d'utilisation interne de l'IA et les principes éthiques. Le domaine **A.3 (Organisation interne)** traite de la structuration de la gouvernance IA : définition des rôles et responsabilités, établissement d'un comité IA ou d'une fonction de gouvernance IA, et mécanismes de reporting. Le domaine **A.4 (Ressources pour les systèmes d'IA)** concerne l'allocation et la gestion des ressources : données d'entraînement, infrastructure de calcul, outils de développement et de monitoring, et compétences humaines spécialisées. Pour approfondir, consultez AI Act 2026 : Guide Conformité Systèmes IA à Haut Risque.

Le domaine **A.5 (Évaluation de l'impact)** impose des processus d'évaluation des impacts des systèmes d'IA sur les individus, les groupes de personnes et la société. Le domaine **A.6 (Cycle de vie du système d'IA)** couvre l'ensemble des phases du cycle de vie : conception, développement, test et validation, déploiement, exploitation et maintenance, et retrait. C'est le domaine le plus granulaire, avec des contrôles dédiés à chaque phase. Le domaine **A.7 (Données pour les systèmes d'IA)** traite de la gouvernance des données utilisées par les systèmes d'IA : qualité, provenance, préparation, étiquetage, et gestion des biais dans les données.



## Annexe B : Objectifs de mise en œuvre

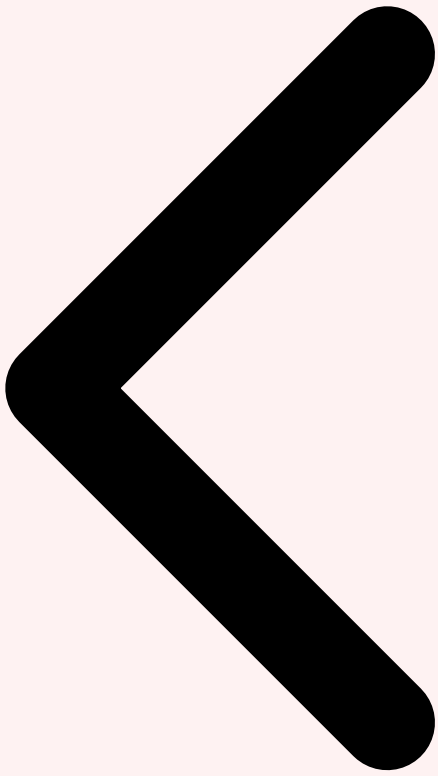
L'Annexe B fournit les **objectifs de mise en œuvre** pour chaque contrôle de l'Annexe A. Alors que l'Annexe A indique « quoi faire », l'Annexe B précise « comment et pourquoi ». Pour chaque contrôle, l'Annexe B décrit l'objectif attendu, les éléments à considérer lors de la mise en œuvre, et les critères d'évaluation de l'efficacité. Par exemple, pour le contrôle A.7 relatif aux données, l'Annexe B détaille les objectifs en matière de qualité des données (exactitude, complétude, cohérence, actualité), de traçabilité (provenance, transformations

appliquées, versions), et de gestion des biais (détection, mesure, mitigation). Cette structure en deux niveaux — contrôles prescriptifs et objectifs de mise en œuvre — offre aux organisations un **cadre à la fois structurant et flexible**, permettant une adaptation aux contextes spécifiques tout en maintenant un niveau d'exigence élevé.

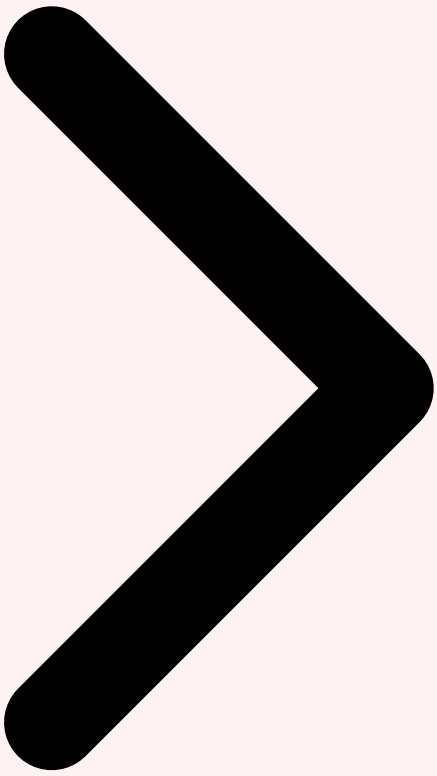
Les domaines **A.8 (Informations pour les parties intéressées)** et **A.9 (Utilisation des systèmes d'IA)** sont particulièrement pertinents dans le contexte de l'AI Act européen. A.8 impose des contrôles de transparence et de communication envers les utilisateurs et les personnes affectées par les systèmes d'IA, incluant l'information sur le fait qu'un système d'IA est utilisé, l'explication des décisions automatisées, et les mécanismes de recours. A.9 traite de la supervision humaine des systèmes d'IA, de la définition des limites d'utilisation, et des procédures de désactivation en cas de dysfonctionnement. Le domaine **A.10 (Relations avec les tiers)** couvre la gestion des relations avec les fournisseurs de technologies IA, incluant la due diligence, les exigences contractuelles, et l'audit des fournisseurs — un sujet critique avec l'essor de API d'IA tierces (OpenAI, Google, Anthropic) massivement utilisées par les organisations.

**Comparaison structurelle : Annexe A ISO 42001 vs Annexe A ISO 27001**

- ●**ISO 27001:2022** — 93 contrôles en 4 thèmes (Organisationnels, Humains, Physiques, Technologiques)
- ●**ISO 42001:2023** — 39 contrôles en 9 domaines (Politiques, Organisation, Ressources, Impact, Cycle de vie, Données, Transparence, Utilisation, Tiers)
- ●**Complémentarité** — Les contrôles ISO 42001 ne couvrent pas la sécurité de l'information (couverte par ISO 27001), mais ajoutent des dimensions spécifiques à l'IA (éthique, équité, transparence, impact sociétal)
- ●**SoA intégrée** — Une organisation certifiée ISO 27001 et ISO 42001 peut maintenir une SoA combinée couvrant les 132 contrôles des deux normes

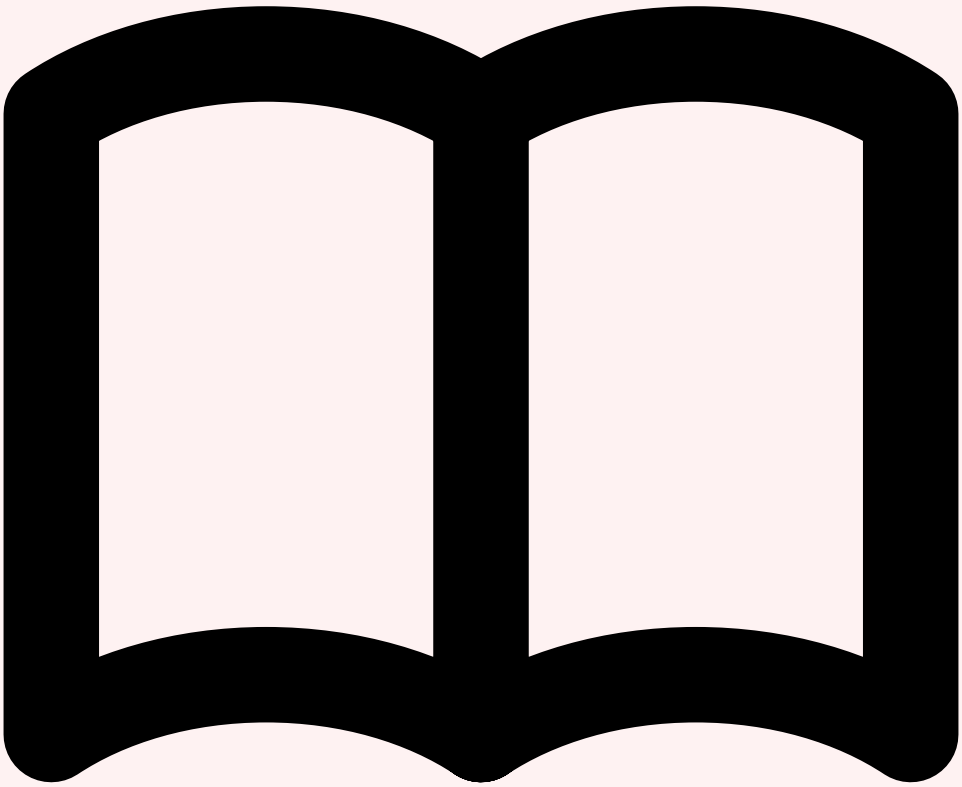


Exigences Opérationnelles (8-10) Annexes A et B Certification PECB Foundation



## 6 Certification PECB ISO/IEC 42001 Foundation

Le **Professional Evaluation and Certification Board (PECB)** est l'un des principaux organismes internationaux de certification des personnes dans le domaine des systèmes de management. Accrédité par des organismes d'accréditation reconnus internationalement, le PECB propose un parcours de certification complet pour l'ISO/IEC 42001, dont le niveau **Foundation** constitue le point d'entrée. Cette certification atteste que le titulaire maîtrise les concepts fondamentaux, la structure et les exigences de la norme ISO/IEC 42001, et qu'il est capable de contribuer efficacement à la mise en œuvre et au maintien d'un SMIA au sein de son organisation.

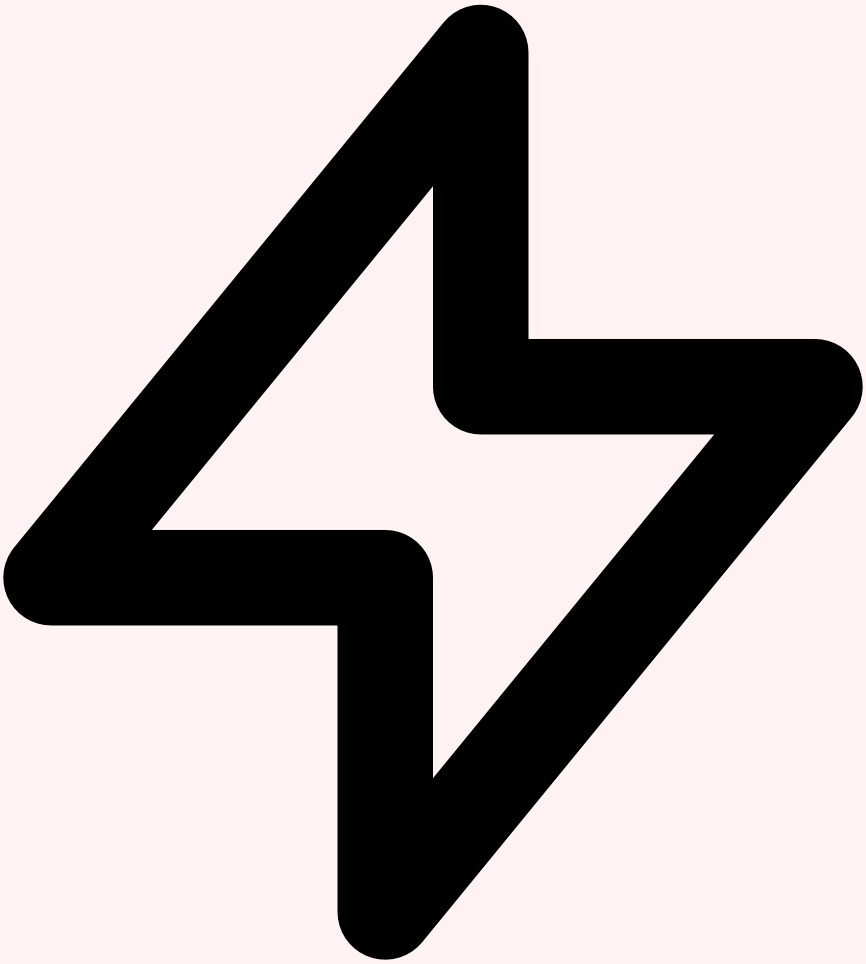


### Programme de formation Foundation

La formation PECB ISO/IEC 42001 Foundation se déroule sur **2 jours (14 heures)** et couvre l'ensemble des concepts nécessaires à la compréhension de la norme. Le programme est structuré en modules progressifs. Le **premier jour** couvre les fondamentaux : introduction à l'intelligence artificielle et aux systèmes de management, historique et contexte de la publication de l'ISO/IEC 42001, présentation de la structure harmonisée (HLS) et du cycle PDCA, analyse détaillée des clauses 4 à 7 (contexte, leadership, planification, support), et exercices pratiques sur la définition du périmètre SMIA et l'élaboration d'une politique IA. Le **second jour** approfondit les clauses opérationnelles (8 à 10), les annexes A et B avec leurs 39 contrôles, les relations avec l'AI Act européen et les autres normes ISO, la préparation à l'examen avec des exercices de simulation, et se conclut par l'examen de certification.

## Structure de l'examen

L'examen PECB ISO/IEC 42001 Foundation est un examen à **livre ouvert (open book)**, d'une durée de 60 minutes, composé de 40 questions à choix multiple. Le score minimum de réussite est de **70 % (28 bonnes réponses sur 40)**. Les questions couvrent cinq domaines principaux, pondérés comme suit : la structure et les exigences de la norme ISO/IEC 42001 (environ 30 % des questions), les contrôles de l'Annexe A et les objectifs de l'Annexe B (25 %), les concepts fondamentaux de l'intelligence artificielle et du management de l'IA (20 %), le cycle PDCA et les principes des systèmes de management (15 %), et les termes et définitions (10 %). Le caractère « livre ouvert » signifie que le candidat peut consulter la norme ISO/IEC 42001 et ses notes de cours pendant l'examen, ce qui déplace l'évaluation de la mémorisation vers la **compréhension et l'application** des concepts.

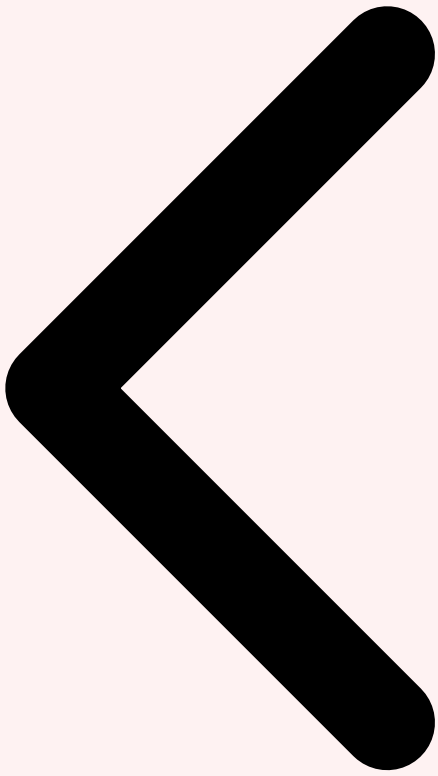


### Conseils de préparation

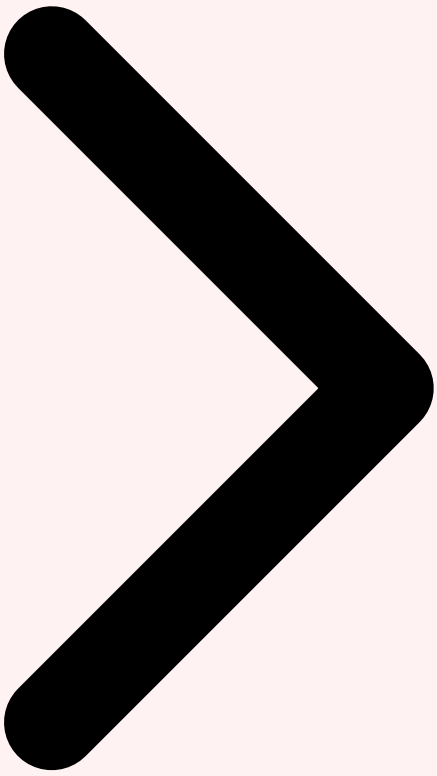
Pour maximiser vos chances de réussite à l'examen Foundation, plusieurs stratégies de préparation sont recommandées. Premièrement, **lisez la norme ISO/IEC 42001 au moins deux fois** avant la formation, en prenant des notes sur les concepts clés et les numéros de clauses. Familiarisez-vous avec la terminologie de l'ISO/IEC 22989 (vocabulaire de l'IA) et les définitions du chapitre 3 de la norme. Deuxièmement, **maîtrisez la structure HLS** : si vous connaissez déjà l'ISO 27001 ou l'ISO 9001, identifiez les éléments communs et concentrez-vous sur les spécificités de l'ISO 42001 (clauses 8.2 à 8.4, annexes A et B). Troisièmement, **préparez votre exemplaire annoté** de la norme avec des onglets ou signets pour retrouver rapidement les clauses et contrôles pendant l'examen. Quatrièmement, entraînez-vous sur les **questions de simulation PECB** disponibles sur la plateforme en ligne, en chronométrant vos réponses pour respecter le rythme de 1,5 minute par question. Enfin, comprenez bien les relations entre les clauses normatives et les annexes : pour chaque exigence des clauses 4 à 10, identifiez les contrôles de l'Annexe A correspondants et les objectifs de l'Annexe B associés.

**Profils cibles de la certification Foundation**

- ●**Responsables conformité** — Comprendre les exigences de l'ISO 42001 pour intégrer l'IA dans le périmètre de conformité
- ●**RSSI et DPO** — Étendre leur expertise aux enjeux spécifiques de gouvernance de l'IA
- ●**Chefs de projet IA** — Intégrer les exigences de management dès la conception des projets IA
- ●**Data scientists et ML engineers** — Comprendre le cadre de gouvernance dans lequel leurs travaux s'inscrivent
- ●**Auditeurs internes** — Acquérir les bases avant la formation Lead Auditor ISO 42001
- ●**Consultants en transformation digitale** — Enrichir leur offre avec une compétence certifiée en gouvernance IA



Annexes A et B Certification PECB Foundation Synergie AI Act et Normes



## 7 Synergie avec l'AI Act et Autres Normes

L'ISO/IEC 42001 n'existe pas en vase clos. Elle s'inscrit dans un **écosystème normatif et réglementaire en pleine structuration** qui inclut le Règlement européen sur l'IA (AI Act), les normes de sécurité de l'information (ISO 27001), les cadres de gestion des risques IA (NIST AI RMF), et un ensemble croissant de standards techniques spécialisés. Comprendre ces interactions est essentiel pour les organisations qui doivent naviguer dans un paysage de conformité multi-dimensionnel.

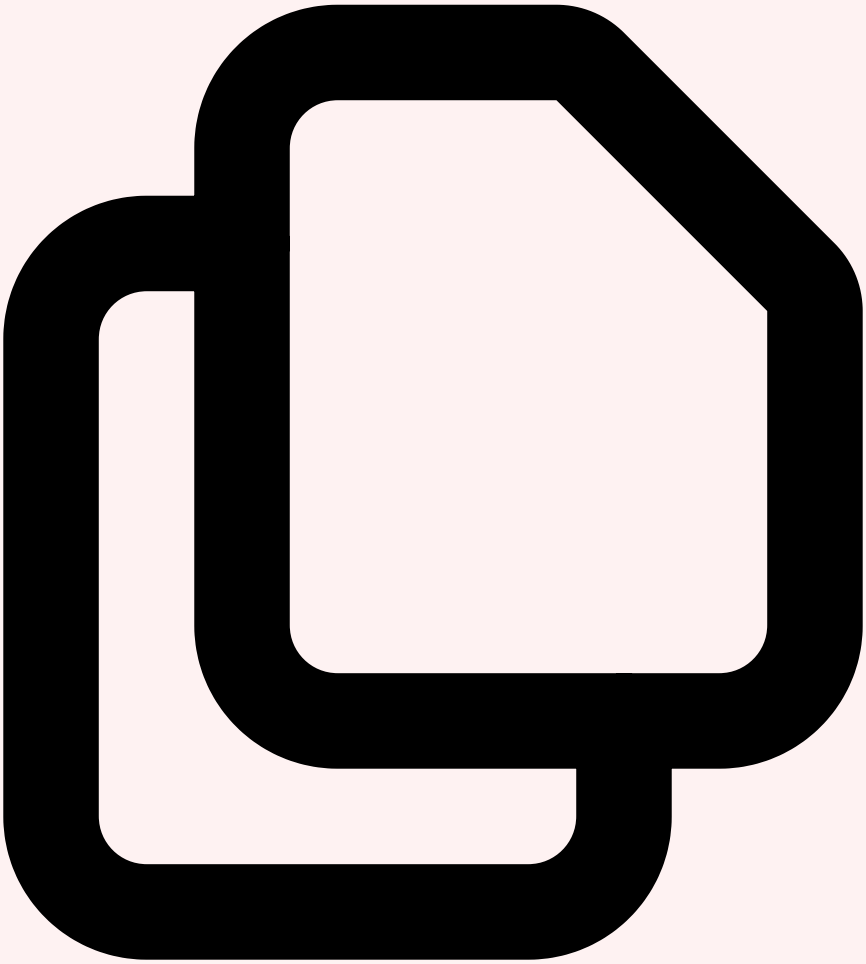
### ISO 42001 et AI Act : la présomption de conformité

La relation entre l'ISO/IEC 42001 et l'**AI Act (Règlement (UE) 2024/1689)** est fondamentale. L'article 40 de l'AI Act établit le principe des **normes harmonisées** : les systèmes d'IA à haut risque qui sont conformes à des normes harmonisées publiées au Journal officiel de l'Union européenne bénéficient d'une présomption de conformité aux exigences du règlement couvertes par ces normes. Le CEN et le CENELEC ont reçu de la Commission européenne un mandat de normalisation (M/593) pour développer ces normes harmonisées, et l'ISO/IEC 42001 — via son adoption européenne potentielle comme EN ISO/IEC 42001 — est la candidate principale pour cette harmonisation sur le volet « système de management ».

Concrètement, pour une organisation qui déploie des **systèmes d'IA à haut risque** au sens de l'Annexe III de l'AI Act (recrutement, scoring de crédit, diagnostic médical assisté, justice prédictive, etc.), la certification ISO 42001 pourrait constituer un élément central de démonstration de conformité aux exigences des articles 9 (gestion des risques), 10 (données et gouvernance des données), 11 (documentation technique), 12 (tenue de registres), 13 (transparence et information des utilisateurs), 14 (contrôle humain), et 15 (exactitude, robustesse et cybersécurité). Cependant, la présomption de conformité n'est pas automatique : elle dépend de la publication formelle de références harmonisées au

JOUE, un processus qui était encore en cours en février 2026. En attendant, la certification ISO 42001 constitue une **preuve forte mais non suffisante** de conformité, que les autorités de marché prendront vraisemblablement en compte dans leurs évaluations. Pour approfondir, consultez Développement Sécurisé ISO 27001 : Cycle S-SDLC en 6 Phases.

| Exigence AI Act | Article | Clause ISO 42001 | Contrôle Annexe A |
|---|---|---|---|
| Système de gestion des risques | Art. 9 | 6.1, 8.2, 8.3 | A.5, A.6 |
| Données et gouvernance | Art. 10 | 8.1, 8.4 | A.4, A.7 |
| Documentation technique | Art. 11 | 7.5 | A.6 |
| Tenue de registres | Art. 12 | 7.5, 9.1 | A.6, A.8 |
| Transparence | Art. 13 | 7.4 | A.8 |
| Contrôle humain | Art. 14 | 8.1 | A.9 |
| Exactitude, robustesse, cybersécurité | Art. 15 | 8.1, 9.1 | A.6, A.7 |

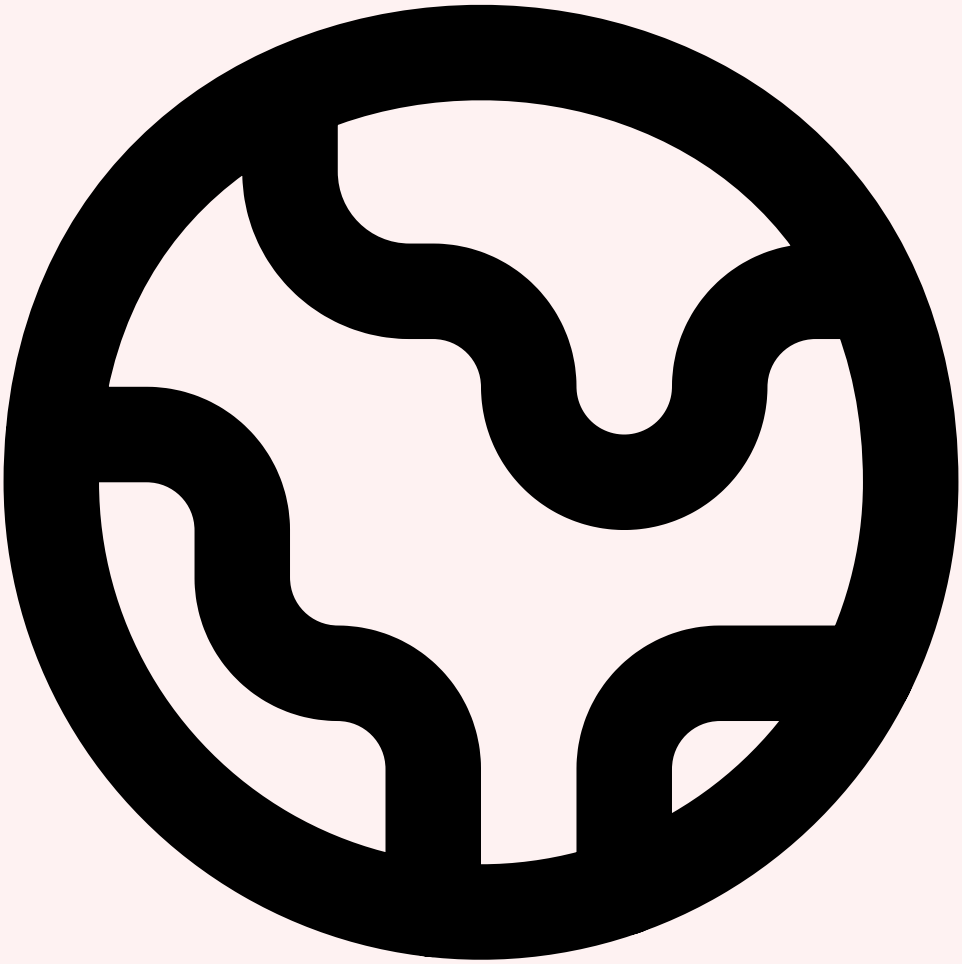


### Intégration avec l'ISO 27001

L'intégration de l'ISO/IEC 42001 avec l'**ISO/IEC 27001:2022** est naturelle et synergique grâce à la structure harmonisée commune. Les organisations déjà certifiées ISO 27001 disposent d'un avantage considérable pour la mise en œuvre de l'ISO 42001 : le cadre de management (gouvernance, documentation, audit interne, revue de direction, amélioration continue) est déjà en place. Les principales extensions nécessaires concernent : l'ajout des **contrôles spécifiques IA** de l'Annexe A de l'ISO 42001 à la SoA existante, l'extension du processus d'appréciation des risques pour couvrir les risques spécifiques à l'IA (biais, dérive, explicabilité, impact sociétal), la mise en œuvre de processus d'**analyse d'impact des systèmes d'IA** (clause 8.4), et l'enrichissement des compétences des équipes sur les dimensions spécifiques de l'IA.

En pratique, un **système de management intégré (SMI)** combinant ISO 27001 et ISO 42001 partage une politique unique (étendue à l'IA), un processus de gestion des risques commun (avec des catégories de risques IA ajoutées), un programme d'audit interne consolidé, et une revue de direction couvrant les deux périmètres. L'audit de certification peut être réalisé simultanément par un organisme accrédité pour les deux normes,

réduisant les coûts et la charge administrative. Plusieurs organismes de certification (BSI, Bureau Veritas, TÜV, SGS, AFNOR Certification) proposent déjà des **audits combinés ISO 27001 + ISO 42001**.



### NIST AI RMF et autres cadres internationaux

Au-delà de l'écosystème européen, l'ISO/IEC 42001 interagit avec d'autres cadres internationaux de gouvernance de l'IA. Le **NIST AI Risk Management Framework (AI RMF 1.0)**, publié en janvier 2023, propose une approche par fonctions (Govern, Map, Measure, Manage) pour la gestion des risques liés à l'IA. Bien que non certifiable, le NIST AI RMF est largement adopté aux États-Unis et ses concepts se retrouvent dans l'ISO 42001 : la fonction Govern correspond aux clauses 4-5 (contexte et leadership), Map aux clauses 6 et 8.4 (planification et analyse d'impact), Measure à la clause 9 (évaluation des performances), et Manage aux clauses 8 et 10 (fonctionnement et amélioration). Les organisations opérant sur les marchés américain et européen peuvent utiliser l'ISO 42001 comme socle commun en l'enrichissant avec les profils spécifiques du NIST AI RMF pour les exigences américaines.

L'écosystème normatif ISO/IEC en matière d'IA continue de s'étoffer avec des normes complémentaires : l'**ISO/IEC 23894** (gestion des risques IA) fournit un cadre détaillé applicable dans le contexte de l'ISO 42001, l'**ISO/IEC 38507** (gouvernance de l'IA pour les organes de direction) aide les conseils d'administration à superviser l'IA, l'**ISO/IEC 25059** (qualité des systèmes d'IA) définit des métriques de qualité spécifiques, et l'**ISO/IEC TR 24027** traite des biais dans les systèmes d'IA. En France, le guide **AFNOR SPEC 2314** sur l'IA de confiance complète ce panorama en proposant des recommandations adaptées au contexte réglementaire français. L'ensemble forme un corpus normatif cohérent dont l'ISO/IEC 42001 constitue la colonne vertébrale, le système de management qui intègre et opérationnalise l'ensemble des exigences.

**Calendrier réglementaire AI Act à surveiller**

- ●**2 février 2025** — Interdiction des pratiques d'IA prohibées (Article 5)
- ●**2 août 2025** — Obligations pour les modèles d'IA à usage général (GPAI)
- ●**2 août 2026** — Obligations complètes pour les systèmes d'IA à haut risque (Annexe III)
- ●**2 août 2027** — Obligations pour les systèmes d'IA intégrés dans des produits réglementés (Annexe I)

La certification ISO/IEC 42001 dès maintenant permet d'anticiper ces échéances et de structurer progressivement la conformité.

## Besoin d'un accompagnement expert ?

Nos consultants en cybersécurité et IA vous accompagnent dans vos projets. Devis personnalisé sous 24h.

### Références et ressources externes

- MITRE ATT&CK T1649 — Steal or Forge Authentication Certificates
- ISO 27001 — Norme internationale de management de la sécurité de l'information
- CNIL — Commission nationale de l'informatique et des libertés
- ENISA — Agence européenne pour la cybersécurité
- EUR-Lex — Portail du droit de l'Union européenne

Pour approfondir ce sujet, consultez notre outil open-source rgpd-compliance-checker qui facilite la vérification automatisée de conformité RGPD.

## Questions frequentes

### Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, installer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

### Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en œuvre de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

### Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

**Sources et références :** CNIL · ANSSI

## Conclusion

Cet article a couvert les aspects essentiels de Table des Matieres, 1 Qu'est-ce que l'ISO/IEC 42001 ?, 2 Architecture de la Norme : Structure Harmonisée et PDCA. La mise en pratique de ces recommandations permet de renforcer significativement la posture de securite de votre organisation.

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr