

Guide pratique

La passerelle

D'ISO 9001 et ISO 27001 vers ISO/IEC 42001.
Ce qui se réutilise, ce qui se repense, et ce qui
n'existait nulle part avant.

Michel Fotsing, CISSP

Auditeur principal ISO/IEC 42001, certifié PECB

Volontaire à la révision des examens de l'ISC2

Auteur de *L'Architecte Numérique*, distribué par Hachette

Septembre 2026

Édition 1.0 · Diffusion libre

SOMMAIRE

Ce que vous trouverez ici.

01	Pourquoi ce guide	3
02	Ce qu'ISO/IEC 42001 demande vraiment	4
03	Votre avantage caché : la structure harmonisée	5
04	Les trois choses qui n'existaient nulle part avant	6
	L'impact sur les personnes	7
	La frontière de délégation	8
	La surveillance de la dérive	9
05	L'Annexe A lue par une organisation 27001	10
06	Ce que le Québec ajoute	11
07	Le plan des 90 jours	12
08	Les cinq erreurs que je vois	13
09	Avant de parler de certification	14

Vos normes actuelles vous demandent de maîtriser vos processus et de protéger votre information. ISO 42001 vous demande, en plus, de répondre de ce que vos systèmes automatisés font aux personnes.

CHAPITRE 01

Publiée en décembre 2023, ISO/IEC 42001 est la première norme certifiable au monde pour un système de management de l'intelligence artificielle.

Elle a été écrite délibérément sur la même structure que 9001 et 27001.

Pourquoi ce guide

Ce document s'adresse à une personne précise : le directeur qualité, le responsable de la sécurité de l'information ou le responsable de la conformité qui a déjà bâti un système de management, qui le fait vivre depuis des années, et qui vient d'apprendre que son organisation déploie de l'intelligence artificielle.

Cette personne a deux réactions à peu près simultanées. La première est de se dire que tout est à refaire. La seconde est de se demander si, au fond, son système existant ne couvrirait pas déjà une bonne partie du terrain.

La seconde intuition est la bonne. C'est ce que ce guide démontre, clause par clause.

Une organisation qui vit déjà avec 9001 ou 27001 possède la charpente, la culture d'audit interne, la revue de direction et la maîtrise documentaire. Elle n'a pas besoin d'apprendre à gérer un système de management. Elle a besoin de savoir précisément ce que l'IA ajoute.

Ce guide fait trois choses. Il cartographie ce qui se réutilise tel quel. Il nomme ce qui doit être adapté. Et il isole les trois exigences qui n'existaient dans aucune norme de management avant 2023, celles où la plupart des organisations découvrent qu'elles n'ont rien.

Ce que ce guide n'est pas

Ce n'est ni un cours accrédité, ni un substitut au texte de la norme, ni une garantie de certification. C'est le carnet de route d'un praticien qui a fait l'exercice pour lui-même et qui l'écrit parce qu'il n'existait pas en français.

CHAPITRE 02

4

ajouts structurels par rapport à 9001 et 27001

Les clauses 4 à 10 portent la même numérotation que celles que vous connaissez déjà.

Ce qu'ISO/IEC 42001 demande vraiment

Une confusion revient sans cesse, y compris chez des gens sérieux : ISO 42001 ne certifie pas un système d'IA. Elle certifie la manière dont une organisation gère ses systèmes d'IA.

La nuance change tout. Un modèle médiocre géré avec rigueur peut être conforme. Un excellent modèle déployé sans cadre ne le sera jamais. Comme pour 9001 et 27001, la norme exige que l'organisation comprenne son contexte, engage sa direction, planifie, se donne les moyens, opère, évalue et s'améliore. Ce qui la distingue tient en quatre ajouts.

L'évaluation d'impact, en plus de l'évaluation des risques

La clause 6.1.4 et l'objectif A.5 introduisent une notion absente de 9001 et 27001 : l'impact des systèmes d'IA sur les personnes, les groupes et la société. Le risque, dans vos normes actuelles, est un risque pour l'organisation. L'impact, ici, est un effet sur des tiers qui n'ont rien signé. C'est le changement de perspective le plus profond de la norme.

Le cycle de vie comme objet de gouvernance

L'objectif A.6 couvre l'ensemble du cycle de vie d'un système d'IA, de la spécification à la mise hors service. Un procédé industriel bien réglé reste réglé. Un modèle, non. La norme en tire les conséquences.

Les données comme ressource gouvernée

L'objectif A.7 traite la donnée d'entraînement, de validation et de test comme une ressource à part entière : acquisition, qualité, provenance, préparation. Pour une organisation 27001, c'est un prolongement naturel de la classification. Pour une organisation 9001 seule, c'est un chantier neuf.

L'usage responsable, y compris par des tiers

Les objectifs A.8 à A.10 couvrent l'information fournie aux parties intéressées et les relations avec fournisseurs et clients. La norme s'applique aussi bien à celui qui développe un système d'IA qu'à celui qui l'achète et l'utilise. La plupart des PME sont dans le second cas, et elles sont tout autant concernées.

CHAPITRE 03

1

Votre avantage caché : la structure harmonisée

seule clause sur sept introduit
une exigence sans équivalent

Depuis 2012, toutes les normes de systèmes de management ISO partagent la même ossature : dix clauses, dans le même ordre, avec les mêmes intentions. Si votre organisation tient un système 9001 ou 27001 vivant, les éléments suivants existent déjà et n'ont pas à être réinventés. Ils doivent être étendus pour couvrir l'IA, ce qui est un travail de quelques semaines et non de plusieurs mois.

Exhibit 1

Ce que vos normes actuelles vous ont déjà donné, clause par clause

Clause	9001 ou 27001 vous a donné	ISO 42001 y ajoute
4. Contexte À ADAPTER	Enjeux internes et externes, parties intéressées, périmètre.	Le rôle de l'organisation face à l'IA (développeur, utilisateur, fournisseur), et les parties touchées par les systèmes d'IA, pas seulement par l'organisation.
5. Leadership À ADAPTER	Engagement de la direction, politique, rôles et responsabilités.	Une politique IA distincte ou intégrée (A.2), des rôles nommés pour la gouvernance de l'IA (A.3).
6. Planification NOUVEAU	Approche par les risques, objectifs, planification des changements.	L'évaluation d'impact des systèmes d'IA (6.1.4). La seule clause de la structure commune qui contient une exigence réellement neuve.
7. Support À ADAPTER	Ressources, compétences, sensibilisation, communication, information documentée.	Compétences spécifiques à l'IA; documentation des ressources de données, d'outillage et de calcul (A.4).
8. Opération À ADAPTER	Planification et maîtrise opérationnelles.	Répéter risques et impact en phase opérationnelle (8.2 à 8.4); gouverner le cycle de vie (A.6).
9. Évaluation À ADAPTER	Surveillance, mesure, audit interne, revue de direction.	Surveiller la performance et la dérive des systèmes en exploitation, pas seulement les indicateurs du système.
10. Amélioration RÉUTILISABLE	Non-conformités, actions correctives, amélioration continue.	Rien de structurellement neuf. Les incidents liés à l'IA entrent dans le processus existant.

Source : ISO/IEC 42001:2023, clauses 4 à 10, lues contre la structure harmonisée ISO. Analyse de l'auteur.

Là où le travail réel se trouve, c'est dans l'Annexe A, et dans trois exigences que le reste de ce guide examine une à une.

Les trois choses qui n'existaient nulle part avant.

Quand on retire de la norme tout ce qui est structure harmonisée et tout ce qui prolonge naturellement 27001, il reste trois exigences que je n'ai vues formalisées dans aucune norme de management auparavant.

Ce sont celles qui demandent le plus de réflexion, et souvent le plus de courage.

PREMIÈRE NOUVEAUTÉ

Clauses 6.1.4 et 8.4

Objectif A.5

Le mot important est *distinct*. Ce n'est pas une ligne de plus dans votre registre de risques. C'est un exercice à part, avec sa méthode et sa documentation.

Le pont avec la Loi 25. Si vous avez déjà mené une EFVP, vous avez fait l'équivalent, restreint aux renseignements personnels. Réutilisez la méthode; élargissez le périmètre.

L'impact sur les personnes

Vos normes actuelles évaluent le risque pour l'organisation. Perte financière, interruption, atteinte à la réputation, non-conformité. ISO 42001 exige une évaluation distincte : l'impact du système d'IA sur les individus et les groupes qui le subissent, et sur la société.

Prenez une usine qui déploie un outil de maintenance prédictive à partir des données de capteurs. Le risque organisationnel est clair : un faux négatif coûte un arrêt de production. Mais l'outil signale aussi des anomalies de comportement d'équipement, et certaines corrélient avec des opérateurs. Le jour où le signalement devient un indicateur de performance individuelle, la question change de nature.

C'est ça, l'impact sur les personnes, et la norme demande qu'il soit évalué avant le déploiement, pas après la première plainte.

Ce que l'évaluation doit contenir

Au minimum : les personnes et groupes touchés, la nature de l'effet, sa gravité, sa réversibilité, les mesures d'atténuation, et la décision motivée de procéder ou non. Elle doit être répétée quand le contexte ou le système change de façon significative.

L'évaluation d'impact d'ISO 42001 est plus large qu'une EFVP : elle inclut les effets qui ne touchent pas la vie privée, comme l'accès à un service, la discrimination ou la sécurité physique.

DEUXIÈME NOUVEAUTÉ**Objectifs A.6 et A.9****Usage prévu A.9.4**

Le tri entre les trois zones n'est pas une préférence philosophique. C'est une décision d'ingénierie et de gouvernance, qui doit être écrite, datée et approuvée.

La frontière de délégation

Aucune norme de management ne vous a jamais demandé d'écrire quelles décisions une machine peut prendre seule. ISO 42001 le fait, sans utiliser ce vocabulaire, à travers les exigences sur l'usage prévu, la supervision humaine et les processus d'usage responsable.

Dans mon propre travail, j'utilise trois zones pour tracer cette frontière.

Exhibit 2**Les trois zones de délégation**

Zone	Qui décide	Rôle de l'humain
Automatisée	Le système décide.	Vérification par échantillonnage.
Augmentée	Le système propose.	L'humain dispose.
Sanctuaire	Le système n'entre pas.	Quelle que soit la performance du système. Un choix organisationnel, fait d'avance et écrit.

Source : cadre des Trois Zones, *L'Architecte Numérique*, 2026.

Ce que la norme attend concrètement : que chaque système d'IA ait un usage prévu documenté, que les cas hors périmètre soient identifiés, et que les mécanismes de supervision humaine soient définis et proportionnés. Une organisation qui ne peut pas répondre à la question « quelles décisions cet outil prend-il seul » ne satisfait pas la norme, même si tout le reste est en ordre.

Le livrable le plus utile que j'ai vu est une charte de délégation d'une page à deux pages, signée par la direction, qui liste les décisions par zone. Elle devient la pièce centrale de l'audit interne.

TROISIÈME NOUVEAUTÉ

Clause 9.1

Contrôle A.6.2.6

75%

Le seuil que j'ai tenu pendant quatre ans, et qui n'était écrit nulle part.

Critères d'acceptation,

A.6.2.4. Avant tout déploiement, la norme attend des critères définis, documentés, approuvés, et la preuve qu'ils ont été atteints. Si vous avez un seuil informel, c'est la première chose à formaliser.

La surveillance de la dérive

Un procédé bien réglé reste bien réglé. Un modèle, non. Les données du monde changent, les comportements changent, et la précision d'un système descend sans que personne ne s'en aperçoive.

La norme exige que l'exploitation d'un système d'IA inclue une surveillance continue de sa performance, et que des seuils déclenchent une réaction.

Pour une organisation 9001, l'analogie la plus juste est la maîtrise statistique des procédés. Vous savez déjà surveiller une dérive de cote sur une ligne de production. Appliquez la même discipline à un modèle : un indicateur de performance défini avant le déploiement, une fréquence de mesure, un seuil d'alerte, et une procédure quand le seuil est franchi.

Ce qui manque le plus souvent n'est pas la mesure, c'est le seuil écrit d'avance. J'ai tenu pendant quatre ans une règle simple sur un système de vision par ordinateur : sous 75 % de précision sur le jeu de test, on ne déploie pas. Cette règle n'était écrite nulle part. Elle vivait dans ma tête et elle est partie avec moi.

C'est exactement ce que la norme vient corriger.

CHAPITRE 05

38

contrôles en neuf objectifs,
appliqués par déclaration
d'applicabilité

L'Annexe A lue par une organisation 27001

Comme dans 27001, vous justifiez les contrôles que vous retenez et ceux que vous écarterez. Pour chaque objectif, ce qu'une organisation 27001 possède déjà et ce qu'elle doit construire.

Exhibit 3

Les neuf objectifs de l'Annexe A : acquis et à construire

Objectif	Nb	Si vous avez 27001	À construire
A.2 Politiques liées à l'IA	3	Une politique de sécurité de l'information et un cycle de revue.	Une politique IA, alignée, revue périodiquement.
A.3 Organisation interne	2	Rôles formalisés; canal de signalement.	Étendre les rôles à l'IA.
A.4 Ressources pour les systèmes d'IA	5	Inventaire des actifs; ressources humaines et techniques.	Documenter données, outillage, calcul et compétences par système.
A.5 Évaluation des impacts	4	Rien de directement équivalent. L'EFVP est le point de départ le plus proche.	Le processus complet : méthode, documentation, impacts individuels et sociétaux. Chantier principal.
A.6 Cycle de vie des systèmes d'IA	9	Développement sécurisé, gestion des changements, journalisation.	Développement responsable, vérification et validation, surveillance en exploitation, journaux d'événements.
A.7 Données pour les systèmes d'IA	5	Classification, propriété des actifs, protection.	Acquisition, qualité, provenance, préparation. Extension de la classification.
A.8 Information pour les parties intéressées	4	Communication, incidents, obligations de notification.	Documentation utilisateur, signalement externe, incidents liés à l'IA.
A.9 Usage des systèmes d'IA	3	Politique d'utilisation acceptable.	Usage responsable, usage prévu documenté par système. La frontière de délégation vit ici.
A.10 Relations avec les tiers et les clients	3	Fournisseurs, clauses contractuelles, évaluation des tiers.	Répartition des responsabilités dans la chaîne de valeur de l'IA.

Source : ISO/IEC 42001:2023, Annexe A, lue contre ISO/IEC 27001:2022. Analyse de l'auteur.

Six objectifs sur neuf sont des extensions de contrôles que vous opérez déjà. Deux sont partiellement couverts. Un seul part de zéro. Pour une organisation 9001 sans 27001, le chemin le plus court passe souvent par une implantation conjointe des deux normes.

CHAPITRE 06**Article 12.1**

Loi sur la protection des renseignements personnels dans le secteur privé

Une décision en zone automatisée déclenche l'article 12.1. Une organisation qui a tracé ses zones sait immédiatement quelles décisions sont visées.

Exposition européenne. Le règlement sur l'IA, en application depuis le 2 août 2026 pour la transparence et à partir de décembre 2027 pour le haut risque, ne demande pas ISO 42001. Mais un SMIA conforme produit précisément la documentation qu'il exige.

Ce que le Québec ajoute

ISO 42001 est une norme internationale et volontaire. Au Québec, elle se superpose à des obligations légales qui, elles, ne sont pas optionnelles. Trois points de contact permettent de faire d'une pierre deux coups.

Les décisions automatisées

L'article 12.1 oblige une organisation qui prend une décision fondée exclusivement sur un traitement automatisé à en informer la personne, à lui donner l'occasion de présenter ses observations, et à lui communiquer sur demande les renseignements utilisés et les principaux facteurs de la décision. Cette obligation cadre exactement avec la frontière de délégation.

L'évaluation des facteurs relatifs à la vie privée

La Loi 25 exige une EFVP pour tout projet impliquant des renseignements personnels. Un système d'IA entraîné ou alimenté avec des données personnelles y est presque toujours assujéti. La bonne pratique consiste à mener l'EFVP et l'évaluation d'impact ISO 42001 comme un seul exercice à deux volets, plutôt que deux documents séparés qui se contredisent six mois plus tard.

Les transferts hors Québec

Un modèle hébergé ou entraîné hors Québec, ce qui est le cas de la plupart des services d'IA générative, constitue une communication de renseignements personnels hors du territoire, avec l'évaluation préalable que la loi exige. Les contrôles A.10 sur les tiers et A.7 sur la provenance des données sont les bons endroits pour documenter cette analyse.

CHAPITRE 07

90

jours pour passer d'un usage non gouverné à un usage gouverné, avec des preuves

Ce plan suppose un système 9001 ou 27001 vivant, et entre un et cinq systèmes d'IA en usage ou en développement.

Après 90 jours. La certification devient une option à évaluer selon le besoin d'affaires, pas une fin en soi. Beaucoup d'organisations s'arrêtent ici, avec raison, jusqu'à ce qu'un client ou un régulateur demande l'attestation.

Le plan des 90 jours

01 Jours 1 à 30 • Voir clair

Inventorier les systèmes d'IA en usage, y compris ceux que les employés utilisent sans autorisation formelle. Cet inventaire surprend presque toujours. Pour chaque système : qui l'utilise, sur quelles données, pour quelles décisions. Étendre le périmètre du système de management existant. Nommer un responsable, même à temps partiel.

Livrable : un inventaire d'une page par système, et une décision de périmètre approuvée par la direction.

02 Jours 31 à 60 • Tracer les frontières

Pour chaque système, écrire l'usage prévu et classer les décisions dans les trois zones. Rédiger la charte de délégation. Mener une première évaluation d'impact sur le système le plus exposé, en réutilisant la méthode d'EFVP élargie. Formaliser les critères d'acceptation et les seuils de surveillance.

Livrable : la charte de délégation signée, une évaluation d'impact complète, et les seuils écrits.

03 Jours 61 à 90 • Faire tenir

Intégrer l'IA dans le programme d'audit interne existant. Ajouter un point IA à la revue de direction. Mettre en place la surveillance de la dérive sur au moins un système. Rédiger la politique IA, ou amender la politique de sécurité existante. Former les responsables de processus concernés.

Livrable : un premier audit interne couvrant l'IA, et la politique approuvée.

CHAPITRE 08

Cinq erreurs observées chez des organisations sérieuses, avec de bons systèmes, qui abordent 42001 pour la première fois.

Les cinq erreurs que je vois

01 Traiter l'évaluation d'impact comme une ligne du registre de risques

L'erreur la plus fréquente, et elle est compréhensible : le registre existe, il est confortable, on y ajoute une ligne. Mais l'impact sur les personnes n'est pas un risque pour l'organisation, et un auditeur le verra immédiatement.

02 Confondre gouverner l'IA et sécuriser l'IA

Les équipes de sécurité lisent 42001 comme un 27001 bis. Une bonne partie leur est familière, mais les objectifs A.5 et A.9 ne sont pas des questions de sécurité. Ce sont des questions de responsabilité et de choix organisationnels. Elles exigent la direction à la table, pas seulement les TI.

03 Documenter sans décider

Une organisation peut produire une politique, un inventaire et une charte sans jamais trancher une seule frontière difficile. La charte qui ne contient que des cas évidents ne vaut rien. Ce sont les cas litigieux, ceux où la direction hésite, qui donnent à la charte sa valeur.

04 Oublier les systèmes achetés

La norme couvre l'utilisation, pas seulement le développement. L'assistant de votre suite bureautique, le module de recommandation de votre CRM, l'outil de tri de candidatures de votre fournisseur RH : tous entrent dans le périmètre. La plupart des PME n'ont aucun système développé à l'interne et sont pourtant entièrement concernées.

05 Viser la certification avant le besoin

La certification a un coût, en argent et en attention. Elle vaut la peine quand un client, un régulateur ou un partenaire l'exige, ou quand elle ouvre un marché. Un SMIA vivant et non certifié vaut mieux qu'un SMIA certifié qui dort dans une armoire.

CHAPITRE 09

Pour aller plus loin. Le cadre des Trois Zones est développé en entier dans *L'Architecte Numérique : Orchestrer les intelligences à l'ère de l'IA*, distribué par Hachette. L'ouvrage traite de la question que ce guide ne fait qu'effleurer : non pas comment documenter la frontière, mais où la tracer.

L'auteur. Architecte en cybersécurité, CISSP, auditeur principal ISO/IEC 42001 certifié par PECB, volontaire à la révision des examens de l'ISC2. Quatre ans comme chef de produit d'une solution de vision par ordinateur en production.

michel@larchitectenumerique.com

Avant de parler de certification

Il y a quelque chose de rassurant à découvrir qu'une norme parue en 2023 formalise des pratiques que des gens raisonnables avaient déjà trouvées, chacun de leur côté, par nécessité.

Les seuils avant déploiement, les décisions qu'on refuse de confier à une machine, la surveillance après la mise en service : rien de tout ça n'est tombé du ciel avec la norme. Mais tout ça reposait sur des personnes. Sur leur jugement, leur rigueur, leur présence. Le jour où elles partent, la pratique part avec elles.

C'est, au fond, ce qu'un système de management vient corriger. Pas de rendre les gens meilleurs. De faire en sorte que ce qu'ils font de bien survive à leur départ.

Si votre organisation tient déjà un système 9001 ou 27001, vous avez fait la moitié du chemin sans le savoir. L'autre moitié tient dans trois exigences et quatre-vingt-dix jours. Ce guide vous donne la carte. Le reste est une question de décision.

Faites-le circuler.

Ce guide peut être partagé, cité et diffusé librement, en entier et sans modification, à condition d'en mentionner l'auteur. Si vous le trouvez utile, transmettez-le à la personne de votre organisation qui en aura besoin.

Pour toute utilisation en formation ou en accompagnement, écrivez-moi.