GUIDE DE PRÉPARATION ISO/IEC 42001

Les informations à réunir avant de lancer votre gouvernance IA

Comment définir le bon périmètre lors d'un atelier de cadrage

SEEGER CONSULTING

www.seegerconsulting.online
contact@seegerconsulting.online
+41 22 575 32 50

Gouvernance IA, continuité d'activité et sécurité opérationelle

Introduction

L'intelligence artificielle est déjà présente dans de nombreuses entreprises, parfois de manière visible, parfois de manière plus discrète.

Elle peut être intégrée dans des outils bureautiques, des logiciels métiers, des plateformes fournisseurs, des solutions documentaires, des outils de cybersécurité, des assistants conversationnels ou des pratiques spontanées des collaborateurs.

Avant de mettre en place une démarche ISO/IEC 42001 ou un système de management de l'intelligence artificielle, il est essentiel de réunir les bonnes informations.

Ce guide aide une direction, un responsable sécurité, IT, conformité, risques ou un chef de projet IA à préparer un premier atelier de cadrage.

Il ne s'agit pas d'évaluer votre entreprise de manière exhaustive. Il s'agit de rassembler les éléments de base qui permettront de comprendre où l'IA est déjà présente, quels usages sont sensibles, quels risques doivent être traités en priorité et quel périmètre pourrait être retenu pour démarrer.

> L'objectif n'est pas la perfection. L'objectif est la visibilité.

Pourquoi ce guide ? À qui s'adresse-t-il ?

Une démarche ISO/IEC 42001 ne doit pas commencer par la rédaction de documents théoriques. Elle doit commencer par une compréhension claire de la réalité de l'entreprise. Ce guide aide à structurer les premières questions, à identifier les informations disponibles et à repérer les zones d'incertitude.

1. Pourquoi préparer ces informations ?

Avoir une vision claire de la situation réelle avant d'entamer toute démarche normative :

- Quels outils IA sont utilisés
- Par quels services
- Avec quelles données
- Pour quelles finalités
- Avec quels fournisseurs
- Sous quelle responsabilité
- Avec quels contrôles
- Avec quels risques

> *"Une direction ne peut pas piloter ce qu'elle ne voit pas."*

2. À qui s'adresse ce guide ?

Fonctions concernées :

- Directions générales
- Responsables sécurité, IT, conformité, risques, achats, RH
- Chefs de projet IA

Contextes d'utilisation :

- Entreprises utilisant déjà des outils IA
- Sociétés développant ou intégrant une solution IA
- Entreprises envisageant une démarche ISO/IEC 42001
- Prestataires souhaitant renforcer la confiance autour de leurs solutions IA

Il peut être utilisé seul, avant une première réunion interne, ou comme support de préparation avant un atelier avec Seeger Consulting.

3. Ce que ce guide n'est pas

- Ce n'est pas un audit ISO/IEC 42001
- Il ne remplace pas une analyse d'écart complète
- Il ne constitue pas une validation juridique, technique ou réglementaire
- Il ne permet pas, à lui seul, de démontrer la conformité d'un système de management de l'IA

Il s'agit d'un outil de préparation, pas d'un rapport de conformité.

Les informations à réunir sur l'entreprise et ses pratiques IA

Avant d'aborder les applications IA elles-mêmes, il est utile de réunir quelques informations générales sur l'entreprise.
La première étape concrète consiste ensuite à recenser les déploiements IA connus.

4. Les informations générales à réunir

À préparer

- nom de l'entreprise
- secteur d'activité
- nombre approximatif de collaborateurs
- pays ou régions d'activité
- principaux clients ou types de clients
- services ou départements concernés par l'IA
- personnes déjà impliquées dans les sujets IA
- existence d'une direction IT, sécurité, conformité, risques ou qualité
- principaux enjeux stratégiques liés à l'IA
- contraintes particulières liées au secteur d'activité

Questions utiles

- L'IA est-elle déjà considérée comme un sujet stratégique ?
- La direction a-t-elle déjà exprimé une position sur le recours à l'IA ?
- Existe-t-il un projet IA officiellement lancé ?
- Existe-t-il plutôt des utilisations dispersées et informelles ?
- Un responsable IA ou un groupe de pilotage a-t-il déjà été désigné ?

5. Les applications IA déjà identifiées

À préparer

- liste des outils IA officiellement autorisés
- liste des outils IA utilisés par certains collaborateurs
- outils IA intégrés dans Microsoft 365, Google Workspace, CRM, ERP ou autres logiciels métiers
- assistants conversationnels utilisés
- outils de génération de texte, traduction, résumé documentaire, analyse de données
- outils de génération d'images, de vidéos ou de présentations
- outils IA déployés en cybersécurité, sécurité physique, RH, marketing, relation client, opérations
- outils IA utilisés par des fournisseurs externes

Questions utiles

- Quels services ont déjà recours à l'IA ?
- Ces pratiques sont-elles connues de la direction ?
- Les outils sont-ils validés par l'IT ou la sécurité ?
- Les collaborateurs savent-ils ce qu'ils peuvent ou ne peuvent pas faire ?
- Existe-t-il des déploiements non déclarés ?

Pratiques sensibles et données traitées par les outils IA

Toutes les applications de l'IA ne présentent pas le même niveau de risque. Les pratiques sensibles doivent être identifiées en priorité. La gouvernance IA commence souvent par une question simple : quelles données sont traitées ?

6. Les pratiques sensibles à identifier en priorité

À préparer

- utilisations impliquant des données personnelles
- applications impliquant des données clients
- recours à l'IA impliquant des informations confidentielles
- déploiements impliquant des contrats ou documents juridiques
- utilisations impliquant des données financières
- applications impliquant des données RH
- recours à l'IA liés à la sécurité ou à la surveillance
- déploiements influençant une décision importante
- utilisations liées à des processus critiques
- applications reposant sur des fournisseurs externes
- pratiques fortement visibles pour les clients ou le public

Questions utiles

- Un outil IA influence-t-il une décision concernant une personne ?
- Un outil IA traite-t-il des informations confidentielles ?
- Un outil IA est-il utilisé pour produire des documents officiels ?
- Un outil IA peut-il avoir un impact sur un client ?
- Un outil IA peut-il générer une erreur difficile à détecter ?

7. Les données utilisées par les outils IA

À préparer

- types de données utilisées
- données personnelles, clients, collaborateurs
- données financières, contractuelles, techniques
- données de sécurité et données stratégiques
- documents internes, mains courantes, rapports, procédures ou historiques d'incidents
- fichiers importés dans des outils IA
- prompts ou requêtes envoyés à des services externes
- résultats produits par les outils IA

Questions utiles

- Les collaborateurs savent-ils quelles données ne doivent jamais être saisies dans un outil IA public ?
- Les données envoyées à un outil IA sont-elles classifiées ?
- Les données sont-elles hébergées en Suisse, en Europe ou ailleurs ?
- Les données peuvent-elles être réutilisées par le fournisseur ?
- Les données peuvent-elles servir à entraîner un modèle ?

Fournisseurs IA et politiques internes existantes

Un fournisseur IA peut devenir un maillon important de la chaîne de confiance. Une démarche ISO/IEC 42001 peut souvent s'appuyer sur des documents déjà en place.

8. Les fournisseurs IA et solutions externes

À préparer

- liste des fournisseurs IA déjà utilisés
- fournisseurs de logiciels intégrant des fonctions IA
- fournisseurs cloud
- fournisseurs de solutions documentaires
- fournisseurs cybersécurité
- fournisseurs sécurité physique
- fournisseurs RH
- fournisseurs marketing
- fournisseurs de traduction ou rédaction assistée
- contrats existants
- conditions générales
- accords de traitement des données
- documentation sécurité
- documentation technique
- lieux d'hébergement
- sous-traitants connus

Questions utiles

- Le fournisseur explique-t-il clairement où les données sont traitées ?
- Le fournisseur indique-t-il si les données servent à entraîner le modèle ?
- Existe-t-il des clauses contractuelles sur la confidentialité ?
- Le fournisseur documente-t-il ses sous-traitants ?
- Existe-t-il une procédure de sortie ou de réversibilité ?

9. Les politiques et documents internes existants

À préparer

- politique de sécurité de l'information
- politique de protection des données
- charte informatique
- code de conduite
- politique d'utilisation des outils numériques
- procédure achats
- procédure de gestion des fournisseurs
- registre des risques
- cartographie des processus
- plan de continuité d'activité
- procédures de gestion de crise
- procédures d'incident
- politique qualité
- règles de classification des données
- procédures RH
- programme de formation interne
- règles relatives au télétravail ou aux outils cloud

Questions utiles

- L'entreprise dispose-t-elle déjà d'un système de management ISO 9001, ISO/IEC 27001, ISO 22301 ou autre ?
- Les documents existants couvrent-ils déjà certains risques liés aux déploiements IA ?
- Existe-t-il une politique spécifique à l'IA ?
- Existe-t-il des règles sur le recours aux outils publics d'intelligence artificielle ?
- Les collaborateurs savent-ils où trouver ces règles ?

10 & 11. Responsabilités internes et risques identifiés

La gouvernance IA exige des responsabilités claires. Il est également utile de préparer une première liste des risques perçus.

10. Les responsabilités internes

À préparer

- personne responsable du sujet IA
- sponsor de direction
- responsable IT
- responsable sécurité
- responsable protection des données
- responsable conformité
- responsable risques
- responsable achats
- responsable RH
- responsables métiers concernés
- personnes pouvant valider les nouveaux outils
- personnes pouvant arbitrer les risques
- personnes chargées de former les collaborateurs
- personnes chargées de traiter les incidents IA

Questions utiles

- Qui décide si un outil IA peut être utilisé ?
- Qui valide les applications sensibles ?
- Qui évalue les fournisseurs ?
- Qui traite les questions relatives aux données ?
- Qui répond aux collaborateurs en cas de doute ?
- Qui porte la responsabilité devant la direction ?

11. Les risques déjà connus ou pressentis

À préparer

- risques de fuite d'informations
- risques liés au Shadow AI
- risques de résultats inexacts
- risques d'hallucination
- risques de biais
- risques liés à la protection des données
- risques de dépendance fournisseur
- risques contractuels
- risques de cybersécurité
- risques de continuité d'activité
- risques réputationnels
- risques liés à la qualité des décisions
- risques liés à l'absence de validation humaine
- risques liés à l'empoisonnement des données
- risques liés aux recours à l'IA non autorisés

Questions utiles

- Un incident IA a-t-il déjà eu lieu ?
- Un collaborateur a-t-il déjà signalé une inquiétude ?
- Un outil IA a-t-il déjà produit un résultat faux ou problématique ?
- Des données sensibles ont-elles déjà été saisies dans un outil non validé ?
- Un client a-t-il déjà posé des questions sur les déploiements de l'IA ?

Formations existantes et incidents signalés

La formation est l'une des premières réponses au Shadow AI. Un système de gouvernance IA doit également permettre de traiter les problèmes.

12. Les formations et sensibilisations existantes

À préparer

- formations IA déjà organisées
- formations sécurité de l'information
- formations protection des données
- formations cybersécurité
- formations conformité
- supports de sensibilisation existants
- communications internes sur l'IA
- règles transmises aux collaborateurs
- FAQ interne
- canal de questions ou signalements

Questions utiles

- Les collaborateurs comprennent-ils les risques liés aux outils IA publics ?
- Savent-ils quelles données ne doivent pas être transmises ?
- Savent-ils quels outils sont autorisés ?
- Savent-ils comment vérifier un résultat IA ?
- Savent-ils à qui s'adresser en cas de doute ?

13. Les incidents, préoccupations et signalements

À préparer

- incidents liés à l'IA déjà identifiés
- erreurs importantes produites par un outil IA
- résultats biaisés ou discriminatoires
- fuites ou suspicions de fuite d'information
- recours à un outil non validé
- réclamations clients
- préoccupations de collaborateurs
- questions RH liées à l'IA
- mécanisme de signalement existant
- procédure de traitement des incidents

Questions utiles

- Existe-t-il un canal pour signaler une préoccupation IA ?
- Les collaborateurs savent-ils qu'ils peuvent signaler un problème ?
- Les incidents IA sont-ils documentés ?
- Les incidents IA sont-ils analysés pour améliorer les pratiques ?
- La direction est-elle informée des incidents significatifs ?

Périmètre, attentes de la direction et des parties prenantes

Il n'est pas nécessaire de couvrir toute l'entreprise dès le départ. Une démarche ISO/IEC 42001 exige un leadership clair et peut devenir un argument de confiance auprès des clients et partenaires.

14. Le périmètre possible pour démarrer

À préparer :

- activité prioritaire
- service concerné
- solution IA stratégique
- produit IA développé ou intégré
- processus métier sensible
- famille d'applications IA
- fournisseur IA prioritaire
- zone géographique
- entité juridique ou opérationnelle
- périmètre déjà maîtrisable

Questions utiles :

- Quel périmètre apporterait le plus de valeur rapidement ?
- Quel périmètre présente les risques les plus importants ?
- Quel périmètre est le plus réaliste pour démarrer ?
- Quelle partie de l'entreprise est prête à s'engager ?
- Le périmètre peut-il être clairement expliqué à un auditeur, un client ou un partenaire ?

15. Les attentes de la direction

À préparer :

- objectifs de la direction
- motivations principales
- attentes clients et réglementaires
- volonté de certification
- besoin de rassurer le marché
- besoin de structurer les pratiques internes
- besoin de réduire le Shadow AI
- besoin d'encadrer les fournisseurs
- besoin de protéger les données sensibles
- niveau d'ambition, ressources disponibles, calendrier souhaité

Questions utiles :

- La direction souhaite-t-elle obtenir une certification ?
- Le projet est-il défensif, réglementaire, commercial ou stratégique ?
- Quel résultat serait considéré comme utile après 30, 60 ou 90 jours ?
- Quels arbitrages devront être faits par la direction ?

16. Les attentes des clients et partenaires

À préparer :

- questions déjà posées par des clients
- exigences contractuelles
- questionnaires fournisseurs reçus
- attentes de donneurs d'ordre
- besoin de transparence
- demandes liées à l'AI Act
- demandes liées à la protection des données
- demandes de traçabilité et d'audit
- besoin de démontrer la maîtrise des déploiements IA

Questions utiles :

- Des clients demandent-ils déjà comment l'entreprise recourt à l'IA ?
- Des partenaires exigent-ils des garanties ?
- Des appels d'offres mentionnent-ils l'IA responsable ?
- La gouvernance IA peut-elle devenir un avantage concurrentiel ?
- Une certification ISO/IEC 42001 renforcerait-elle la crédibilité commerciale ?

Premières décisions à préparer et tableau de synthèse

Un atelier de cadrage doit permettre de prendre ou préparer des décisions. Avant un premier atelier, vous pouvez résumer votre situation dans le tableau suivant.

17. Les premières décisions à préparer

À préparer

- faut-il nommer un responsable IA ?
- faut-il créer un groupe de pilotage ?
- faut-il interdire certains outils ?
- faut-il valider une liste d'outils autorisés ?
- faut-il rédiger une politique IA courte ?
- faut-il former rapidement les collaborateurs ?
- faut-il évaluer certains fournisseurs en priorité ?
- faut-il créer un registre des risques IA ?
- faut-il définir un périmètre pilote ?
- faut-il engager une analyse d'écart ISO/IEC 42001 ?

Questions utiles

- Quelles décisions peuvent être prises immédiatement ?
- Quelles décisions exigent l'arbitrage de la direction ?
- Quelles décisions doivent attendre une analyse plus complète ?
- Quelles décisions permettraient de réduire rapidement les risques ?

18. Tableau de préparation synthétique

Thème	Informations disponibles	Informations manquantes	Personnes à impliquer	Priorité
Pratiques IA connues				Élevée
Données traitées				Élevée
Fournisseurs IA				Moyenne
Politique IA				Élevée
Risques IA				Élevée
Formation				Moyenne
Périmètre initial				Basse

Documents à préparer et résultats attendus d'un atelier de cadrage

Si disponibles, les documents suivants peuvent être utiles avant un atelier. Il n'est pas nécessaire de tout avoir. L'absence d'un document est déjà une information utile. Après avoir réuni ces éléments, un premier atelier de cadrage peut permettre de produire des livrables simples et actionnables.

19. Les documents utiles à préparer avant un atelier

- organigramme
- cartographie des processus
- liste des applications métiers
- liste des fournisseurs IT ou IA
- politique de sécurité de l'information
- politique de protection des données
- charte informatique
- procédure achats
- procédure de gestion des fournisseurs
- registre des risques
- plan de continuité d'activité
- procédure de gestion des incidents
- programme de formation
- politique qualité
- documents contractuels fournisseurs
- liste des projets IA en cours
- liste des outils IA autorisés ou utilisés

20. Résultat attendu d'un premier atelier de cadrage

- une vision initiale des pratiques IA
- une identification des principaux risques
- une première liste d'outils sensibles
- une première cartographie des parties prenantes
- une proposition de périmètre SMIA
- une liste d'actions prioritaires
- une première feuille de route
- une décision sur la suite de la démarche
- une estimation des efforts nécessaires
- une clarification des responsabilités

Le bon état d'esprit et comment Seeger Consulting peut vous accompagner

21. Le bon état d'esprit

La gouvernance IA ne doit pas être abordée comme un exercice purement documentaire. Elle doit aider l'entreprise à reprendre la maîtrise de ses déploiements IA, à protéger ses données, à encadrer ses fournisseurs, à former ses collaborateurs et à renforcer la confiance.

> ISO/IEC 42001 donne une structure. La direction donne l'impulsion. Les collaborateurs donnent la réalité du terrain. Les experts apportent la méthode. L'IA peut assister la démarche. L'humain doit en garder la maîtrise.

22. Comment Seeger Consulting peut vous accompagner

Seeger Consulting accompagne les entreprises dans la préparation, le cadrage et la mise en œuvre progressive d'un système de management de l'intelligence artificielle selon ISO/IEC 42001. L'approche proposée est pragmatique, progressive et adaptée à la réalité de l'entreprise. Le but n'est pas de produire de la documentation pour la documentation. Le but est de construire une gouvernance IA utile, compréhensible et applicable.

- Analyse initiale des pratiques IA
- Identification du périmètre pertinent
- Préparation d'une politique IA
- Structuration des responsabilités
- Création d'un registre des risques IA
- Évaluation des fournisseurs
- Sensibilisation des collaborateurs
- Réduction du Shadow AI
- Préparation d'une déclaration d'applicabilité
- Préparation des audits internes
- Préparation d'une démarche de certification