

Gouverner l'intelligence artificielle avec confiance

Guide pratique pour comprendre ISO/IEC 42001
et mettre en place une gouvernance IA responsable

*Comment transformer les opportunités
de l'intelligence artificielle en valeur durable
tout en maîtrisant les risques ?*



Pascal Seeger



Seeger Consulting



www.seegerconsulting.online

LIVRE BLANC



Mentions

Auteur	#####
Date	####
Contact	#####@##### #####

**NOTE DE PRUDENCE** — Les informations contenues dans ce document sont confidentielles et peuvent être soumises à des restrictions d'usage. Elles ne doivent pas être diffusées à l'extérieur de l'entreprise sans l'autorisation préalable du service juridique. Toute utilisation non autorisée est strictement interdite et pourra être sanctionnée. Les informations sont fournies sous réserve d'exactitude et de complétude. Elles ne constituent pas une garantie ou une assurance. Les informations sont fournies à titre informatif uniquement. Elles ne doivent pas être utilisées pour prendre des décisions commerciales ou financières. Les informations sont fournies sous réserve d'exactitude et de complétude. Elles ne constituent pas une garantie ou une assurance. Les informations sont fournies à titre informatif uniquement. Elles ne doivent pas être utilisées pour prendre des décisions commerciales ou financières.

Résumé exécutif

Le présent document a pour objet de résumer les points clés de la réunion tenue le 15/05/2024. Les participants ont discuté des enjeux liés à l'usage de l'IA dans notre entreprise et ont convenu de mettre en place des mesures de protection des données sensibles. Les actions à mener ont été définies et attribuées à des responsables.

Les points abordés lors de la réunion sont les suivants :

- Identification des usages IA déjà présents dans notre entreprise.
- Réduction du Shadow AI par des règles simples et une formation rapide.
- Protection des données sensibles.
- Clarification des responsabilités.
- Évaluation des fournisseurs IA.
- Maintenance d'une validation humaine sur les usages sensibles.
- Définition d'un périmètre réaliste pour démarrer.

Les décisions prises sont les suivantes :

- Adoption d'un cadre de référence pour l'usage de l'IA.
- Mise en place d'un comité d'éthique de l'IA.
- Organisation de sessions de formation pour tous les collaborateurs.
- Renforcement des contrôles de sécurité des données.

Les prochaines étapes à suivre sont :

- Finaliser le cadre de référence pour l'usage de l'IA.
- Recruter les membres du comité d'éthique de l'IA.
- Organiser les sessions de formation.
- Mettre à jour les politiques de sécurité des données.

**À RETENIR POUR LA DIRECTION**

- Identifier les usages IA déjà présents
- Réduire le Shadow AI par des règles simples et une formation rapide
- Protéger les données sensibles
- Clarifier les responsabilités
- Évaluer les fournisseurs IA
- Maintenir une validation humaine sur les usages sensibles
- Définir un périmètre réaliste pour démarrer

Sommaire

Chapitre 1	Pourquoi la gouvernance de l'IA devient un sujet stratégique
Chapitre 2	Opportunités et principaux risques de l'intelligence artificielle
Chapitre 3	Pourquoi ISO/IEC 42001 ? — La norme de management de l'IA
Chapitre 4	Les bénéfices d'une gouvernance IA structurée
Chapitre 5	Les grandes étapes de mise en œuvre d'un SMIA
Chapitre 6	Les erreurs fréquentes à éviter dans une démarche de gouvernance IA
Chapitre 7	Les questions à poser à un fournisseur de solutions IA
Chapitre 8	Comment débiter simplement avec ISO/IEC 42001
Chapitre 9	Pourquoi agir maintenant ?
Chapitre 10	Ce qu'un CEO doit retenir
Chapitre 11	Les premières actions à engager dans les 30 jours

L'IA et les champignons : une analogie éclairante

#####

"L'enjeu n'est pas d'interdire l'IA, mais d'éviter qu'elle ne se développe comme des champignons après la pluie : sans cadre, sans visibilité et sans maîtrise."

#####

Introduction

#####

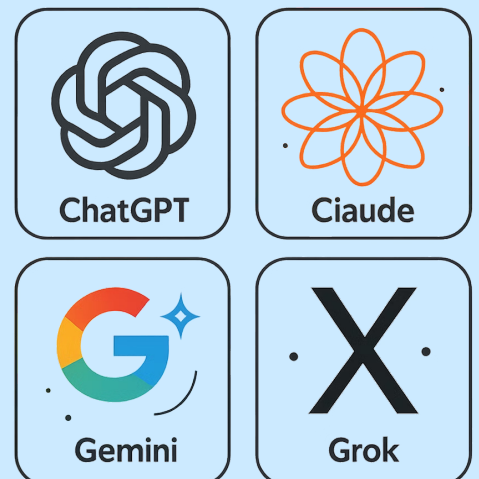
#####

La question centrale

#####

"L'IA ne manque pas de puissance. Elle manque parfois de confiance."

#####



Pourquoi l'IA devient un sujet stratégique

#####

#####

L'IA entre dans tous les métiers

#####

La confiance comme facteur de différenciation

#####

Le défi du Shadow AI

#####

La métaphore des champignons

#####

Un sujet de direction

#####



"#####
#####"

Opportunités de l'IA

#####.

Productivité

#####.

Décision

#####.

Innovation

#####.

Compétitivité

#####.

L'IA comme exosquelette intellectuel

— '#####'

#####.

Elle augmente, elle ne remplace pas

#####.

Elle porte la charge cognitive

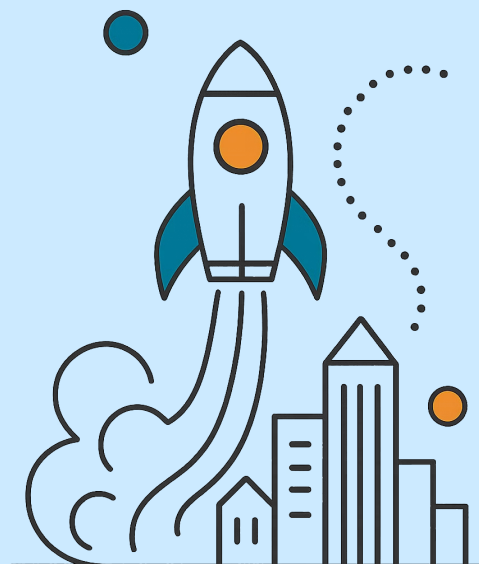
: #####
#####.

Elle ne décide pas à votre place

— #####
#####.

"#####. #####

#####."



Principaux risques de l'IA

#####. #####. #####. #####. #####. #####.

Risques éthiques et de biais

#####,

#####.

Fuite d'informations sensibles

#####,

#####.

Hallucinations et résultats inexacts

#####.

Data poisoning

#####.

Dépendance fournisseur et continuité d'activité

#####,

#####.

Perte de maîtrise humaine

#####.

Shadow AI

#####,

#####,
à #####
—
#####,

#####.

Shadow AI : le risque invisible

**** ***** #'*** ***** ***** ***** ***** ***** ##'**. ## **** ***** *** ##
***** *****.

***** ## ***** #'***** ## **** ***** #'*****
##'***** ***** ***** ***** ## ***** ## ***** ## ****
***** ***** *** ***** *** ***** ***** ## ***** *****.

Ce que cela implique

***** **** ## *****
***** **** *****. ## *****
***** ## **** ## ***** ***
*****. ## ***** *****
***** **** *****.

Ce que cela révèle

##'***** ## ***** ## *****
***** ## ***** à *****
***** *****
***** #'***** *****
***** ***** ## ****
***** **** ## *****
***** ***** ***** ****
***** ***** *****.

Les risques concrets du Shadow AI

Divulgarion d'informations sensibles

***** ***** , ***** , ***** ## , *****
***** ## ***** #'***** ***** **** ## *****
*****.

Juridictions étrangères

***** ## ***** ***** **** ## **** **** ## **** ##
***** ***** ***** ## ***** *****
*****.

Réutilisation des données

***** à ## ***** **** ## ***** ***** **** *****
***** **** ***** **** ## ***** **** ***** ## ****
*****.

Outils hétérogènes incontrôlés

***** #'***** ## ***** , ***** ## ***** à
***** ## ***** ## ***** à ***** ##
*****.

Absence de traçabilité

***** ***** ## **** ***** ***** , ## *****
***** ## **** ***** *****.

Comment réduire le Shadow AI ?

01

Proposer des alternatives sûres

***** ## **** #'***** ***** **** ## ***** ***** ##
***** *****. ## ***** ***** ## ***** ##
***** ***** ## *****.

02

Former rapidement

***** ***** **** ## ***** , ## ***** ***** ##
***** ***** ***** ***** **** ***** **** *****.

03

Créer un canal de signalement

***** ## ***** ## ***** ## ***** #'***** *****
***** ## ***** , **** ***** ## ***** ***** *****.



Pourquoi ISO 42001 ?

#####



Reconnaissance internationale

#####



Cadre de confiance

#####



Approche systémique

#####

Ce que la norme apporte concrètement

Une norme de management, pas une norme produit

#####

Un périmètre progressif

#####

Une logique fondée sur les risques

#####

Un cadre compatible avec d'autres référentiels

#####

Ce qu'un dirigeant suisse doit retenir

#####



#####



Bénéfices d'une gouvernance IA structurée

#####

Confiance renforcée

#####

Réduction du Shadow AI

#####

Protection des données sensibles

#####

Sécurisation des fournisseurs

#####

Innovation responsable

#####

Intégration aux systèmes existants

#####



#####

Intégration avec ISO 9001, ISO 27001 et ISO 22301

#####

ISO 9001 – Qualité

#####

ISO 27001 – Sécurité de l'information

#####

ISO 22301 – Continuité d'activité

#####

Ce que l'intégration permet concrètement

Capitaliser sur l'existant

#####

Réduire les coûts

#####

Gagner du temps

#####

Renforcer la cohérence globale

#####

Processus communs réutilisables	Application à la gouvernance IA
Gestion documentaire	#####
Audits internes	#####
Revue de direction	#####
Gestion des fournisseurs	#####
Gestion des incidents	#####
Amélioration continue	#####

L'IA peut assister la démarche. L'humain doit en garder la maîtrise.

Les grandes étapes de mise en œuvre d'un SMIA

#####.

#####.

01

Cadrer la démarche

##. ##### ## ##### ##,

#####.

02

Obtenir l'engagement de la direction

#####. ## ##### ##### ##

#####.

03

Définir le périmètre

#####.

04

Inventorier les usages IA

##.

05

Évaluer les risques et impacts

#####.

06

Définir les mesures de maîtrise

#####.

07

Former et sensibiliser

##. #####

#####.

08

Auditer, revoir et améliorer

#####. ## #####

##.

09

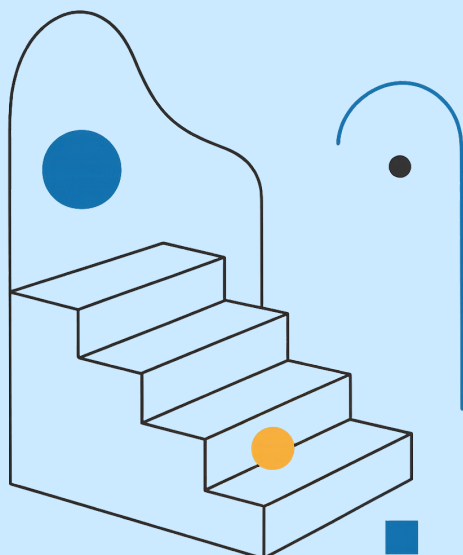
L'IA comme accélérateur de mise en œuvre

#####. ##
#####.



#####. ##### ##

#####.



Les erreurs fréquentes à éviter

#####

Lancer des projets IA sans cadre clair

#####

Croire que l'IA est seulement un sujet IT

#####

Oublier les collaborateurs

#####

Négliger les données

#####

Faire confiance trop vite aux résultats

#####

Choisir des fournisseurs sans analyse

#####

Produire trop de documentation sans impact réel

##

Viser la certification trop tôt

#####

Rôle du leadership

#####. ##### ##### ##
#####.

Ce que la direction doit porter

#####. #####
#####. ## #####
#####. #####
#####.

Ce que la direction doit exiger

#####. ### #####
#####. ###
#####. ###

#####.



PRIORITÉS CEO

1. Porter le projet au niveau de la direction
2. Approuver la politique IA
3. Valider le périmètre du SMIA
4. Arbitrer les risques acceptables
5. Former rapidement les collaborateurs
6. Exiger une validation humaine sur les usages sensibles



L'IA est déjà dans l'entreprise

#####, ## ##

#####, ### #####

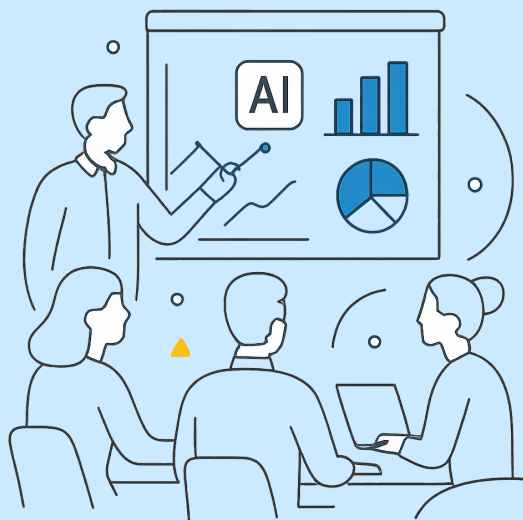
#####.



Un périmètre progressif est possible

##, ###
#####, ## #####
— ##
#####.

#####.



Formation des collaborateurs

#####.

01

Sensibilisation générale

à ## ##### ##
#####.

02

Formation métier

#####.

03

Formation spécialisée

#####.

Questions à poser à un fournisseur IA

#####

→ 1. Comprendre la finalité

#####

→ 2. Comprendre les données

#####

→ 3. Évaluer la sécurité et les sous-traitants

#####

→ 4. Vérifier la qualité des résultats

#####

→ 5. Maintenir la validation humaine

#####

→ 6. Prévoir incidents, continuité et sortie

#####



Avant de signer : #####

#####

Comment démarrer en 30 jours

#####

- 1

Semaine 1

#####
- 2

Semaine 2

#####
- 3

Semaine 3

#####
- 4

Semaine 4

#####

Les 8 actions clés du démarrage

1. Partir des usages réels

#####
2. Réaliser un inventaire simple

#####
3. Identifier les usages sensibles

#####
4. Poser quelques règles immédiates

#####
5. Identifier les outils autorisés

#####
6. Sensibiliser rapidement les collaborateurs

#####
7. Nommer un responsable ou groupe de pilotage

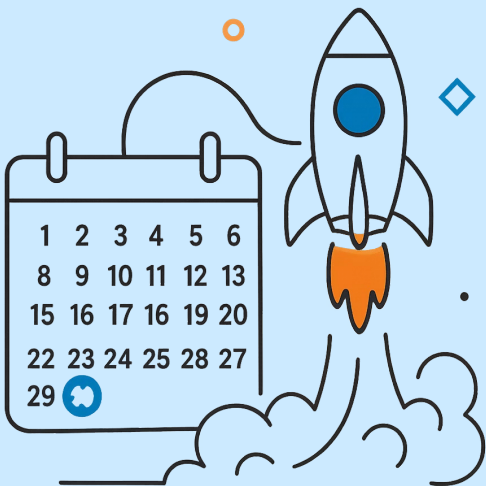
#####
8. Construire un premier registre des risques

#####

□

Après 30 jours

#####



Ce qu'un CEO doit retenir

#####. ## ##### ##### ## #####.

L'IA est un sujet de direction
##. ## ##### ##

#####.

Le cadre existe

#####. ## ##### ##
##.

Agir maintenant

#####. ##### ## ##### ##### ##
#####.

L'humain au centre
#####. ##### ## ##
#####. ##### ## #####

#####.

Les 6 points essentiels pour la direction

1. L'IA est déjà dans l'entreprise
#####, ## ##### ##
#####, ##

#####.

2. Le leadership est déterminant
#####, #####
#####, ##### ## ##### ##

##, ##### ##, ##### ## ##
#####.

3. La formation réduit rapidement le Shadow AI
##,

#####, #####

#####.

4. Les fournisseurs IA doivent être évalués
##,

#####. ## ##### ##### ##### ##
##.

5. La validation humaine reste indispensable
#####, #### ## #####
#####. ## #####
#####.

6. Le périmètre peut être progressif

##, ## #####, ## #####, ## #####, ##
#####, ## ## #####.

 **PRIORITÉS CEO**

- Porter le projet au niveau de la direction
- Approuver la politique IA
- Valider le périmètre
- Arbitrer les risques acceptables
- Former rapidement les collaborateurs
- Exiger une validation humaine sur les usages sensibles

Pourquoi agir maintenant ?

#####

La Suisse avance vers une approche ciblée

#####

L'Europe fixe déjà le rythme

#####

Les clients poseront de plus en plus de questions

#####

Le Shadow AI progresse déjà

#####

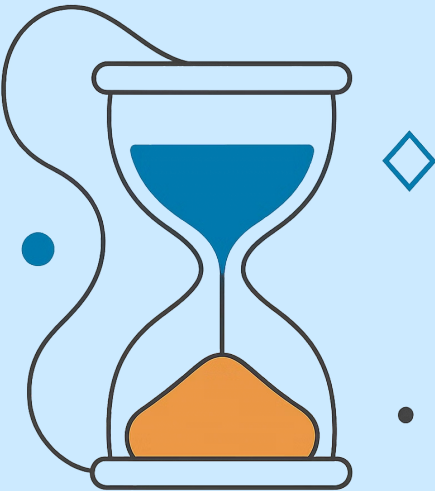
Les fournisseurs intègrent l'IA dans leurs solutions

#####

Le coût de correction peut être élevé

#####

#####



Le rôle du Lead Implementer ISO/IEC 42001

|| #####,

#####

DISTINCTION IMPORTANTE

Lead Implementer : #####

Organisme certificateur : #####

Entreprise : #####

- ## #####

#####





Conclusion

#####

#####

Elle #####

#####

#####

À propos de Seeger Consulting

#####.

Notre expertise

#####.

#####.

Notre approche

#####,
#####,

#####.

Parlons de votre gouvernance IA

?
#####.

Démarrez votre démarche ISO 42001

#####.

L'IA peut assister la démarche

#####.



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

Annexe 1 | Check-list de départ ISO 42001

#####

Thème	Question de départ	Statut
Visibilité sur les usages IA	### ##### ## ##### ##### ## ### ##### ##### ## ### ##### ##### ?	Oui / Non / Partiel
Périmètre initial	## ##### ### ##### ##### ?	Oui / Non / Partiel
Leadership	## ##### ##### ## ##### ##### ?	Oui / Non / Partiel
Politique IA	### ##### ##### ?	Oui / Non / Partiel
Données	### ##### ##### ##### ?	Oui / Non / Partiel
Fournisseurs	### ##### ##### ##### ?	Oui / Non / Partiel
Risques IA	## ##### ## ##### ?	Oui / Non / Partiel
Shadow AI	### ##### ##### ##### ?	Oui / Non / Partiel
Formation	### ##### ##### ### ##### ?	Oui / Non / Partiel
Validation humaine	### ##### ##### ?	Oui / Non / Partiel
Signalement	## ##### ##### ?	Oui / Non / Partiel
Amélioration continue	##### ##### ?	Oui / Non / Partiel

Annexe 2 | Mini-glossaire IA et gouvernance

Terme	Définition synthétique
IA	##### #####, #####, #####, ##### ### # ##.
Système IA	#####, #####, #####, #####, #####.
SMIA	#####.
ISO/IEC 42001	##### ###.
Périmètre du SMIA	#####.
Gouvernance IA	#####, #####, #####, #####, ## #####.
Shadow AI	#####, ##### #####.
Hallucination	#####, #####, ##### #####.
Biais	##### #####.
Data poisoning	##### #####.
Validation humaine	##### #####.
Déclaration d'applicabilité	#####, ##### #####.
AI Act	#####, ##### #####.
NIST AI RMF	#####.
Exosquelette intellectuel	#####, #####.

Annexe 3 | Références et cadres utiles

#####

Référence	Finalité	Utilité dans un projet SMIA
ISO/IEC 42001	Système de management de l'IA	##### #####
ISO/IEC 22989	Concepts et terminologie IA	##### #####
ISO/IEC 23894	Gestion des risques IA	##### ###
ISO/IEC 42005	Évaluation d'impact IA	##### #####
ISO/IEC 24028	Confiance dans l'IA	##### #####
ISO/IEC 23053	Cadre ML	##### #####
ISO/IEC 38507	Gouvernance IA	##### #####
ISO/IEC 27001	Sécurité de l'information	##### #####
ISO 22301	Continuité d'activité	##### #####
ISO 9001	Management de la qualité	##### ##### #####
AI Act européen	Cadre réglementaire IA de l'UE	##### #####
Approche suisse	Cadre national évolutif	##### #####
NIST AI RMF	Cadre volontaire de gestion des risques	##### #####