GOUVERNANCE DE L'IA 2026

AI Act, pilotage des risques et mise en production responsable

Mettre la conformité, la performance et la supervision au service de l'industrialisation des systèmes d'IA.

DaTask

LIVRE BLANC

Avril 2026

POURQUOI LA GOUVERNANCE IA CHANGE-T-ELLE D'ÉCHELLE ?

Du modèle au système, puis du système au système agentique

Hier

On gouvernait surtout un modèle ou un projet : finalité, données, performance, risques.

Aujourd'hui

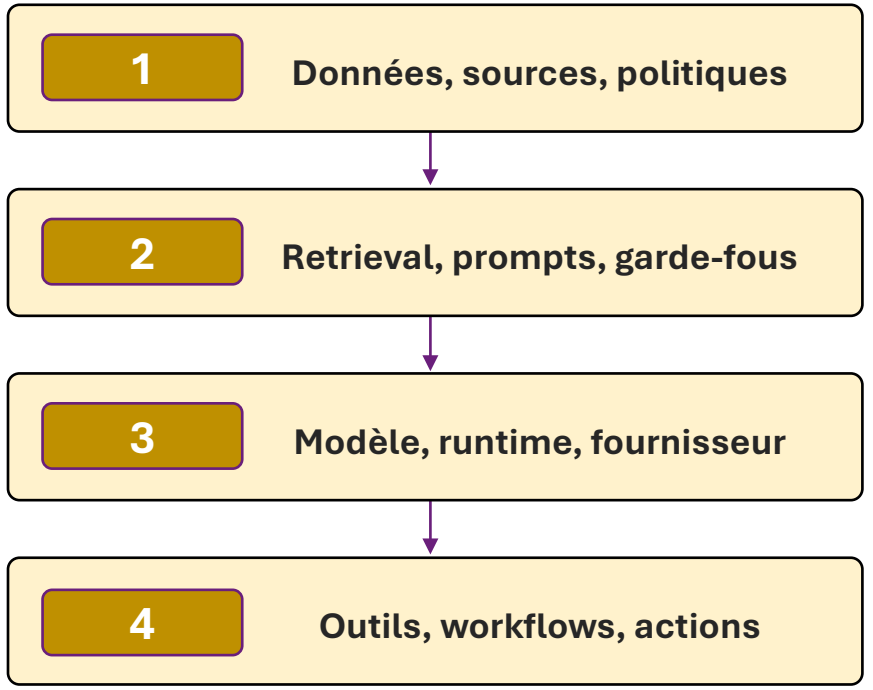
On gouverne un système : données, prompts, retrieval, modèle, fournisseurs, outils, utilisateurs et opérations.

Demain

On gouvernera des agents capables de planifier, d'appeler des outils, de prendre des décisions locales et d'agir dans le SI.

Questions centrales de gouvernance

Qui décide ? Qui contrôle ? Qui prouve ? Qui arrête ?
Plus l'IA agit, plus la gouvernance doit être explicite.



La gouvernance doit suivre toute la chaîne, pas seulement le modèle.

MENACES “SUR” ET IMPACTS “DU” SIA

Quels enjeux de management pour les Systèmes d’Intelligence Artificielle ?

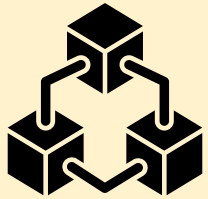
Menaces “sur” le SIA

- Accès non autorisés, exfiltration, compromission.
- Poisoning, attaques adversariales, prompt injection.
- Vulnérabilités logicielles et supply chain.
- Escalade de privilèges via outils et automatisations.
- Dérive des performances, indisponibilité, coûts.

DSI · RSSI · sécurité · architecture

Le système d’IA

à gouverner



Impacts “du” SIA

- Décisions erronées, biais, opacité, faible explicabilité.
- Impacts sur droits, sécurité, sûreté et réputation.
- Effets métier : qualité de service, conformité, litiges.
- Mauvaise supervision humaine et dépendance excessive.
- Propagation d’erreurs à grande échelle dans les opérations.

Métier · risk · legal · audit · ops

2026 : le rôle de l’AI Governance Officer : relier cybersécurité, conformité, métier et exploitation.

UN SIA N’EST PAS UN SYSTÈME COMME UN AUTRE

Trois conséquences directes pour une juste gouvernance

Aspect	Application classique	Système d’IA
Construction	Code et règles explicites.	Données, modèle, prompts, garde-fous, outils.
Production	Comportement plutôt stable.	Drift, hallucinations, changements de modèle ou de fournisseur.
Responsabilité	Chaîne de décision plus simple.	Responsabilité distribuée entre plusieurs acteurs et couches.
Preuves	Tests logiciels et sécurité.	Dossier de gouvernance, journaux, supervision et revues.

1. **Qualifier**
   Le système, son role, ses risques et sa finalité.

2. **Documenter**
   Les preuves, les paramètres et les changements.

3. **Superviser**
   L’usage réel, les incidents et les mises à jour.

Passer d’une logique “projet” à une logique “actif à gouverner”.

LE SYSTÈME À GOUVERNER À L'HEURE DE L'IA EN PRODUCTION

Cycle de vie, composants et questions d'audit

Cycle de vie du SIA

1. **Initialisation**
   Objectifs, exigences, qualification initiale.
2. **Conception**
   Architecture, données, prompts, outils, sécurité.
3. **Vérification**
   Tests, qualité, robustesse, biais, critères d'acceptation.
4. **Déploiement**
   Mise en prod, droits, garde-fous, journalisation.
5. **Exploitation**
   Monitoring, incidents, performance, changements.
6. **Retrait**
   Archivage, effacement, continuité, désactivation.

Questions d'audit à instruire

- Qui conçoit, qui valide, qui supervise, qui exploite ?
- Quelles données entrent, d'où viennent-elles et avec quels droits ?
- Quel modèle, quel runtime, quel fournisseur, quelles dépendances ?
- Quels prompts système, quels garde-fous et quels niveaux d'accès ?
- Quelle traçabilité des événements, incidents et changements ?
- Qui mesure la performance réelle et sur quels seuils d'alerte ?

RAG, prompts, outils et fournisseurs complètent désormais le périmètre initial de la gouvernance IT et Data.

GOVERNANCE BY DESIGN

Sécuriser, documenter, anticiper

Sécuriser

- Scénarios de risque dès le cadrage.
- Dépendances, accès et moindre privilège.
- Robustesse, tests, prompt injection.
- Change control et plan de repli.

Documenter la performance

Finalité et critères d'acceptation.
Biais, qualité, précision, robustesse.
Journaux, incidents, monitoring.
Dossier de preuves pour le go-live.

Anticiper les impacts

Impacts métier, droits, sûreté, réputation.
Supervision humaine et usage réel.

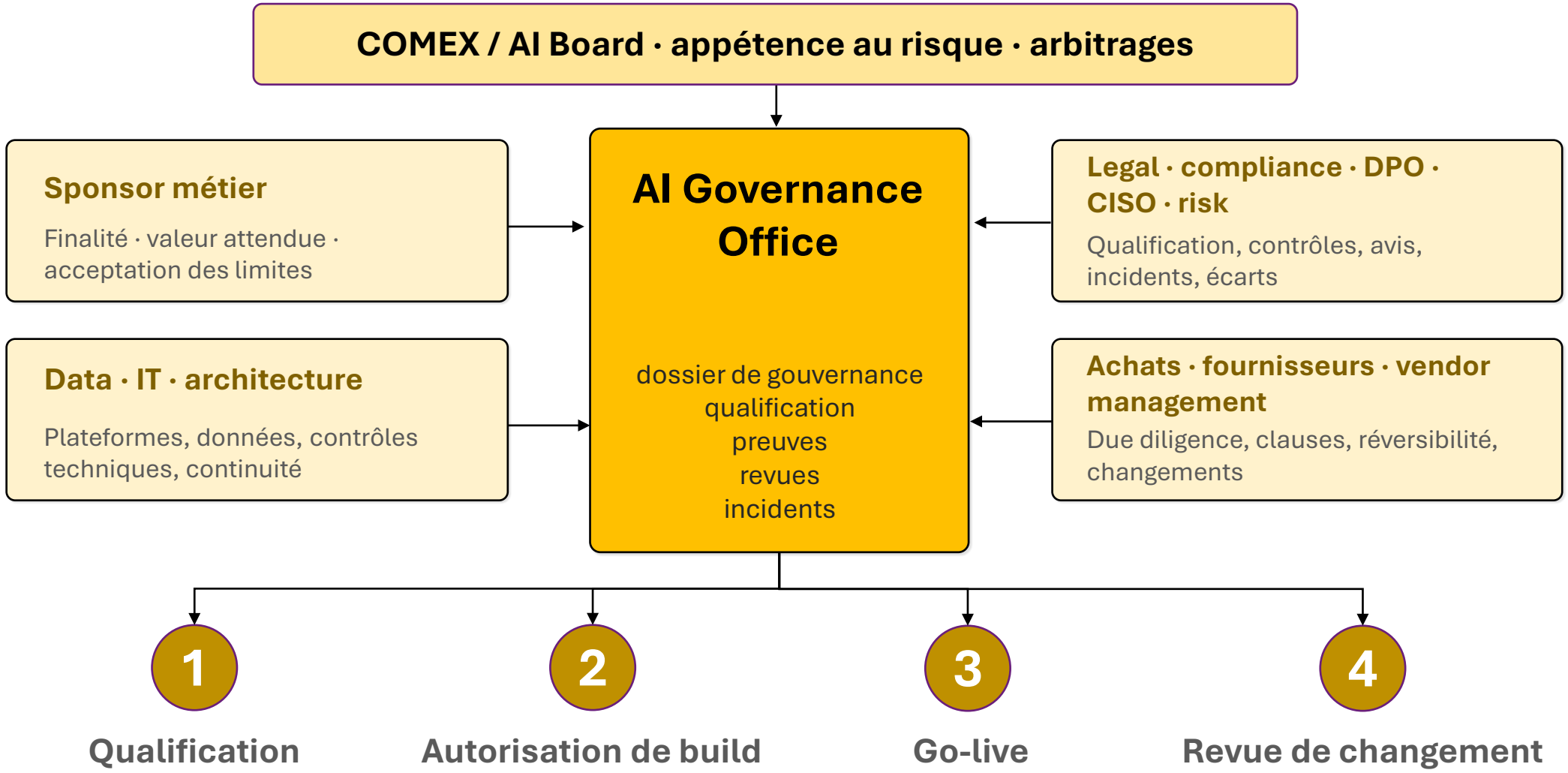
Fournisseurs, coûts, continuité.

Trajectoire AI literacy et adoption.

Décider tôt coûte moins cher que corriger tard : la gouvernance doit être intégrée au design, pas ajoutée après coup.

OPERATING MODEL DE GOUVERNANCE IA

Des rôles clairs et quatre décisions formelles



LE DOSSIER DE GOUVERNANCE PAR CAS D'USAGE

Aucun cas d'usage en production sans système de preuves

1. **Finalité, owner, sponsor**
   Pourquoi le système existe et qui le porte.
2. **Qualification AI Act et rôle tenu**
   Provider, deployer, intégrateur, tiers.
3. **Cartographie des données, modèles et fournisseurs**
   Périmètre technique, dépendances, contrats.
4. **Analyse de risques et d'impacts**
   Cyber, métier, droits, réputation, sûreté.
5. **Plan de tests et critères d'acceptation**
   Qualité, biais, robustesse, sécurité.
6. **Supervision humaine, mode dégradé, arrêt**
   Qui surveille, qui intervient, comment stopper.
7. **Journalisation, monitoring, incidents**
   Événements, seuils d'alerte, remontées.
8. **Change control, revues périodiques, retrait**
   Versions, modifications substantielles, sortie.
9. **AI literacy des personnes concernées**
   Former selon les rôles, le risque et le contexte.

Gouverner l'IA, c'est produire un dossier, pas seulement une opinion.

AI ACT : CALENDRIER UTILE 2025-2027

Ce qui est déjà applicable et ce qui structure la trajectoire

2 fév. 2025
Pratiques interdites
+ AI literacy

2 août 2025
GPAI et règles
de gouvernance

2 août 2026
Applicabilité générale
du règlement

2 août 2027
Certains systèmes à haut risque
intégrés à des produits régulés
+ GPAI déjà sur le marché avant
02/08/2025

Ce que cela implique maintenant en fonction de l'existant

- Inventorier les cas d'usage et les qualifier si ce n'est pas déjà fait.
- Distinguer provider / deployer / intégrateur.
- Lancer la trajectoire AI literacy et les preuves.
- Gouverner les modèles tiers, les changements et les incidents.

Règlement (UE) 2024/1689

AI ACT : OBLIGATIONS PAR RÔLE

Provider, deployer, intégrateur : la première question est la bonne qualification

Provider

- Gérer les risques, la qualité et la documentation.
- Préparer la conformité et les preuves requises.
- Assurer les logs, le monitoring et le suivi post-market.
- Informer via instructions et documentation.
- Traiter les incidents et mesures correctives.

Déployer

- Utiliser conformément à la finalité et aux instructions.
- Assurer la pertinence des données d'entrée.
- Mettre en œuvre la supervision humaine.
- Former les équipes et organiser l'escalade.
- Remonter incidents, risques ou dysfonctionnements.

Intégrateur / vendor management

- Mener la due diligence fournisseur.
- Cadrer sécurité, audit, PI, réversibilité.
- Qualifier les changements et dépendances.
- Gouverner modèles tiers, prompts, outils.
- Préparer plans de repli et options de sortie.

La chaîne de responsabilité peut évoluer si le système est substantiellement modifié : la qualification doit être revue.

RISQUES ET CONTRÔLES DES IA GÉNÉRATIVES, RAG ET AGENTS

Passer d’une typologie d’attaques à une logique de maîtrise

Données & RAG

Risques

- Fuite documentaire
- Poisoning / contamination
- Mauvaise provenance
- Droits d’usage

Contrôles

- Catalogue des sources
- Filtres et ACL
- Versioning
- Rétention / purge

Modèle & prompts

Risques

- Prompt injection
- System prompt leakage
- Unsafe output
- Hallucination

Contrôles

- Revue des prompts
- Guardrails
- Évaluations
- Policies d’usage

Outils & agents

Risques

- Excessive agency
- Misuse des outils
- Abus de privileges
- Chaînage d’actions

Contrôles

- Moindre privilège
- Allowlists
- Sandbox
- Approval gates

Run & fournisseurs

Risques

- Drift
- Incident
- Lock-in fournisseur
- Coût / disponibilité

Contrôles

- Monitoring
- Rollback
- Scorecards
- Exit plan

AI LITERACY : UNE OBLIGATION DE GOUVERNANCE

Former selon les rôles, le niveau de risque et le contexte d'usage

Trois messages clés

- L'obligation s'applique depuis le 2 février 2025.
- Il n'existe pas de programme unique : il faut adapter par rôle, risque et contexte.
- Une trace interne des actions menées suffit ; aucun certificat type n'est imposé

Dirigeants	finalité · appétence au risque · arbitrages
Métiers & owners	usage attendu · limites · impacts · escalade
Builders / data / IT	prompts · sécurité · évaluations · changements
Ops / support terrain	supervision humaine · fallback · journaux · incidents

Les instructions d'utilisation seules sont souvent insuffisantes : la compréhension concrète des risques et du bon usage doit être organisée.

CADRES UTILE POUR STRUCTURER LA GOUVERNANCE

Réglementation, management, impact, sécurité

Réglementation & conformité

AI Act · FAQ AI literacy · GPAI Q&A · Code of Practice · AI Office / Service Desk

Management & impact

ISO/IEC 42001 · 23894 · 42005 · 42006 · 38507

Maîtrise technique

NIST AI RMF GenAI Profile · MITRE ATLAS · OWASP LLM 2025 · OWASP Agentic 2026

Principe

Aucun cadre ne suffit seul.
Il faut articuler :

- droit
- organisation
- impact
- sécurité
- preuves
- audit

ISO/IEC 42001:2023 — Technologies de l'information — IA — Système de management / ISO/IEC 23894:2023 — Technologies de l'information — IA — Recommandations relatives au management du risque / ISO/IEC 42005:2025 — Technologies de l'information — IA— Évaluation de l'impact des systèmes d'IA / ISO/IEC 42006:2025 — Technologies de l'information — IA— Exigences pour les organismes procédant à l'audit et à la certification des systèmes de gestion de l'IA/ ISO/IEC 38507:2022 —Gouvernance des technologies de l'information — Implications de gouvernance de l'utilisation par des organisations de l'IA

GAINS POUR UNE ORGANISATION

Là où la gouvernance IA crée immédiatement de la valeur

1. **Exploitation critique**
   Routing, ETA, allocation, capacités, entrepôts, documents.
2. **Relation client & contenus**
   Support, chat, traduction, knowledge base, documentation.
3. **Données & conformité internationales**
   Confidentialité, transferts, sanctions, traçabilité.
4. **Fournisseurs & modèles tiers**
   Dépendances, coûts, réversibilité, changements de version.
5. **Résilience opérationnelle**
   Cyber, incidents, mode dégradé, continuité d'activité.

Le gouvernance relie

Métier
↕
Risk / legal
↕
Data / IT
↕
CISO
↕
Achats / fournisseurs

Gouvernance = accélérer l'industrialisation sans découvrir le risque trop tard tout en tirant parti des opportunités.

DaTask

Jean-Philippe Riant

AI Governance · Transformation digitale & data

Transport · industrie · banque · défense

jp@riant.fr
+33 (0)6 09 18 65 82
Paris