Définir une gouvernance de l'IA et une organisation claire

Objectif : Mettre en place un cadre décisionnel, éthique et organisationnel pour piloter les projets IA.

Actions clés :

- Nommer un responsable IA (AI Officer / CDO) et définir un comité de gouvernance IA (IT, métiers, juridique, RH).
- Définir une charte d'usage responsable de l'IA (éthique, RGPD, transparence).
- Cartographier les rôles et responsabilités (data scientists, ML engineers, métiers sponsors).
- Mettre en place une procédure de validation des projets IA (priorisation, conformité, ROI attendu).

Outils / Bonnes pratiques :

- RACI pour clarifier les rôles.
- Modèles de politiques IA (par ex. NIST AI Risk Management Framework, ISO/IEC 42001).
- Registre des cas d'usage IA validés.

Indicateurs de succès :

- % de projets IA ayant un sponsor métier identifié.
- % de cas d'usage IA validés par le comité avant déploiement.
- % de conformité aux règles internes et réglementaires.

---

1) Cadre de gouvernance et organisation (qui décide quoi, quand, et comment)

1.1. Rôles clés et organes

- AI Officer / CDO : définit la politique IA, arbitre les priorités, porte les KPI d'adoption et de conformité ; décide des Go/NoGo avec le Comité. Aligner ce mandat sur Leadership & Policy (cl. 5) d'ISO/IEC 42001 et la fonction GOVERN du NIST AI RMF. 1234
- Comité de gouvernance IA (Mensuel, 90'), multi-disciplinaire : IT, Métiers sponsors, Juridique/DPO, Sécurité (CISO), RH/Formation, Data/ML, Achats/Tiers. REX utile : mise en place d'un AI Office avec Chief AI Officer et relais communautés (Présentation savoir fair IA onepoint; Démo Neo & AI Office_PRO BTP). 56
- Sous-comités / "desks" (as needed) : Risk & Compliance (AI Act/RGPD), Architecture & Sécurité, Ethique & UX, Change & Skills. Voir l'axe

"IA Office – industrialisation et gouvernance" (REX marché) (Bouygues - Echange Industrialisation de l'IA).

1.2. Rituels & décisions

- Weekly triage (30'): revue des idées/cas d'usage entrants (formulaire unique, scoring).
- Monthly board : arbitrages, priorisations, levées de risques, Go/NoGo.
- Quarterly review : portefeuille, ROI, conformité, capacité équipes.

Ces rituels correspondent aux fonctions MAP → MEASURE → MANAGE du NIST AI RMF (cadrage risque, mesures, pilotage) et aux exigences de planification & amélioration continue d'ISO 42001 (cl. 6–10).

---

2) Charte d'usage responsable (contenu minimal & ancrage réglementaire)

2.1. Sections recommandées (10 clauses)

1. Objectifs & périmètre (IA/GenAI, agents, data & outils couverts).
2. Principes d'IA responsable (équité, sécurité, transparence, responsabilité) — cohérents avec les principes enseignés dans AI-900T00-PowerPoint_01.fr-FR.
3. RGPD by design : bases légales, minimisation, information des personnes, PIA/AIA quand nécessaire — alignement avec les recommandations CNIL 2024–2025.
4. AI Act (calendrier & catégories de risque) : interdictions, haut risque, GPAI ; intégrer les jalons d'application 2025–2027 dans les contrôles internes.
5. Sécurité & PSSI : classification données, secrets, clés, journalisation, revue tiers — s'aligner sur la Politique de sécurité des systèmes d'information (PSSI).
6. Transparence & traçabilité : cartes de modèles, fiches de jeux de données, registres de prompts.
7. Supervision humaine : boucles HUM-in-the-loop proportionnées au risque (cf. ISO 42001 "human oversight").
8. Propriété intellectuelle & contenus (sources, licences, watermark).
9. Bonnes pratiques de prompt & data hygiene (pas d'infos sensibles hors périmètre contrôlé). Recommandations CNIL & AI Office interne.
10. Mesure & sanctions internes : écarts, remédiations, revues trimestrielles.

---

3) Cartographier rôles & responsabilités (RACI générique IA/GenAI)

À adapter pour chaque cas d'usage ; base alignée sur ISO 42001 (rôles organisationnels) et pratiques AI Office.

Activité / Artefact	Métier Sponsor	PO/ PM	Data Scientist	ML Eng.	Data Eng.	Sec/ CISO	DPO/ Juridique	Ops/ IT	AI Officer/ CDO
Idéation & valeur	**A/R**	R	C	C	C	I	I	I	C
Évaluation risque (AI Act/ RGPD)	C	C	I	I	I	**C**	**A/R**	I	C
Architecture & sécurité	I	C	C	**A/R**	**C/R**	**A/R**	I	C	C
Data sourcing & gouvernance	C	C	C	I	**A/R**	C	**C**	I	C
Expérimentations/ évals	I	C	**A/R**	**R**	C	C	I	I	I
Charte & communication	**A/R**	R	I	I	I	C	**C**	I	C
Mise en prod & MLOps	I	A	C	**R**	**R**	C	I	**A/R**	I
KPI & ROI	**A/R**	**R**	C	C	I	I	I	I	C

Légende : A = Accountable, R = Responsible, C = Consulted, I = Informed.

4) Procédure de validation des projets IA (stage-gates & contrôles)

Gate 0 – Intake & triage (weekly)
Formulaire unique (cf. trame ci-dessous) + scoring Impact/Complexité/Risque → file d'attente comité. Référentiels : NIST RMF MAP ; AI Office (flux d'idéation/priorisation).

Gate 1 – Conformité & risque
- Catégorisation AI Act (interdit/haut/limité/minimal) + mesures associées ; inclure cases GPAI.
- RGPD : base légale, PIA/AIA si nécessaire, minimisation, information. Guides CNIL 2024-2025.

Gate 2 – Architecture & sécurité
- Schéma de flux, classification des données, secrets management, stratégie RAG, isolation/tenants, journaux. S'aligner avec la PSSI et les patterns Azure adoptés dans tes REX (RAG, chunking, stockage souverain) (Description REX DATAIA).

Gate 3 – Expérimentation contrôlée
- Protocole d'évaluation : métriques qualité (précision, groundedness), risques (prompt-leak, jailbreak), red teaming, model cards & data sheets. Adossé à NIST AI RMF Playbook.

Gate 4 – ROI & scale
- Business case (heures économisées, revenus, risques évités) ; coûts (licences, GPU, intégrations, MLOps).
- Plan d'industrialisation (MLOps, supervision, HIL, runbook, SLA).

Gate 5 – Go/NoGo Comité
- Décision formalisée (motifs, dérogations, contrôles compensatoires), inscription au registre, plan de déploiement & change (formations AI Office/Viva Engage).

Gate 6 – Post-déploiement & amélioration continue
- Revue 30/60/90 jours (qualité, dérives, incidents, adoption), continuous compliance (audits légers ISO 42001).

5) Outils & bonnes pratiques (templates prêts à l'emploi)

5.1. Formulaire d'Intake (à mettre dans Forms/SharePoint)

5.2. Registre des cas d'usage IA (extraits – tableur ou liste SharePoint)

Champs minimum : ID, Nom, Sponsor, Catégorie risque (AI Act), Finalité RGPD, Base légale, Données (type/sensibilité), GPAI (oui/non), Évaluations (PIA/AIA), Décision Comité, Contrôles (HIL, logs, safety), Environnements, Intrants/Sortants, Métriques qualité, Incidents, Date de revue prochaine.

S'aligne aux exigences de traçabilité (ISO 42001) et aux bonnes pratiques NIST.

5.3. Politique & référentiels

- NIST AI RMF 1.0 + profil GenAI 2024 (AI 600-1) pour structurer le risk management.
- ISO/IEC 42001:2023 pour formaliser l'AIMS (AI Management System) et les audits internes.
- AI Act : intégrer le timeline d'application dans vos contrôles (prohibitions Fév. 2025 ; GPAI, gouvernance, pénalités Août 2025 ; obligations haut-risque 2026).
- RGPD / CNIL : décliner les "how-to" CNIL (finalité/contrôleur/base légale/ minimisation).

---

6) Indicateurs de succès (définitions, calculs, cibles)

À consolider mensuellement dans un tableau de bord AI Office (Power BI), avec revue trimestrielle au Comité.

Adoption & sponsoring

- % projets IA avec sponsor métier identifié = projets avec Sponsor ≠ N/A ÷ projets totaux (mois). Cible : ≥ 95%.
- % cas d'usage validés par le Comité avant déploiement = cas déployés avec Gate 5 validé ÷ cas déployés. Cible : 100%.
- Taux d'adhésion utilisateur = utilisateurs actifs / ciblés sur 30j (par produit). Cible : ≥ 60% à M+3.
-

Conformité & risque

- % conformité aux règles internes & réglementaires = (# contrôles OK sur checklist ISO 42001 + NIST + RGPD + AI Act) ÷ # contrôles applicables. Cible : ≥ 90%.
- # incidents sécurité/privés (mensuel) et MTTR (heures). Cible : ↓ tendancielle ; MTTR < 24h.
- Couverture AIA/PIA = # cas nécessitant AIA/PIA couverts ÷ # cas éligibles. Cible : 100%.

Valeur & performance

- ROI net (12 mois) = (bénéfices quantifiés – coûts totaux) / coûts totaux.
- Qualité : groundedness, exactitude, taux d'escalade HIL, satisfaction. Référencer le protocole d'évaluation NIST Playbook.

7) Plan 0–90 jours d'implémentation

- S0–2 : Lancer – Nommer l'AI Officer intérim et former le Comité ; adopter les trames Intake et Registre ; publier la v1 de la Charte (2 pages) sur l'intranet AI Office (Viva Engage/SharePoint).
- S3–5 : Outiller – Mettre en place la liste SharePoint "Registre IA", le weekly triage et le monthly board ; intégrer la PSSI & RGPD aux contrôles ; publier le guide "Prompt & Data Hygiene".
- S6–8 : Piloter – Appliquer la procédure sur 2–3 cas pilotes (un GenAI RAG, un prédictif) ; conduire PIA/AIA ; évaluer avec les métriques NIST.
- S9–12 : Étendre – Valider le modèle opérationnel, former relais métiers (via AI Office), fixer les cibles KPI 12 mois, planifier l'audit interne ISO 42001-like.

8) Livrables "clé en main" à produire

1. Terms of Reference du Comité (mandat, pouvoirs, cadences, quorum, modèle de décision).
2. Charte d'usage responsable (v1 synthèse, v2 détaillée).
3. Matrice RACI (par défaut + spécifique par use-case).
4. Procédure stage-gates (intake → GoLive → run).
5. Registre des cas d'usage IA (SharePoint/Excel) + journal des décisions.
6. Kit conformité : checklists AI Act/RGPD, trame PIA/AIA, model card/data sheet. S'appuyer sur : ISO-IEC - 42001-2023 , ISO-IEC - 42001-2023

9) Trames prêtes à l'emploi

9.1. Matrice RACI par type de risque (AI Act) Cf point n°3

Pourquoi cette approche est robuste ?

- Référentiels internationaux éprouvés (NIST AI RMF, ISO/IEC 42001) pour l'organisation, le risque et l'amélioration continue.
- Calendrier AI Act intégré pour éviter les surprises 2025–2027 (prohibitions, GPAI, gouvernance, pénalités).
- Ancrage RGPD & CNIL pour la conformité opérationnelle et la pédagogie auprès des équipes.

REX internes (AI Office, PSSI, gouvernance agents IA) pour accélérer l'adoption concrète dans ton écosystème.