Matrice Enjeu × Contrôle

Positionnez tout projet IA en deux questions

Q1 - ENJEU *Si ce système se trompe ou s'arrête - que se passe-t-il ?*

Q2 - CONTRÔLE *Est-ce qu'on maîtrise ce qu'on met en place ?*

Guide méthodologique

Comment utiliser la matrice- questions, critères, pièges

1. POURQUOI CETTE MATRICE ?

En réunion, quelqu'un propose un outil IA. Tout le monde acquiesce. Personne ne pose les vraies questions. Cette matrice donne deux réflexes : évaluer ce qui se passe si ça échoue, et vérifier qu'on peut en sortir si nécessaire. Elle se remplit en 5 minutes, avant de décider - jamais après.

2. LES DEUX AXES

« Si ce système se trompe ou s'arrête - que se passe-t-il ? »

ENJEU (axe vertical)

Élevé si :

impact sur des personnes · obligation réglementaire (IA Act, RGPD, HDS) · responsabilité juridique · continuité d'activité bloquée

Faible si :

gêne ou perte de productivité · aucune obligation légale · aucun impact sur des tiers

« Est-ce qu'on maîtrise ce qu'on met en place ? »

CONTRÔLE (axe horizontal)

Élevé si :

on comprend comment ça fonctionne · on peut l'auditer · clause de sortie dans le contrat · données exportables · alternative identifiée

Faible si :

boîte noire · fournisseur unique · pas de clause de sortie · données verrouillées · juridiction étrangère applicable

3. LES 4 ZONES ET CE QU'ELLES IMPLIQUENT

	Signal	Ce qu'il faut faire
CONFORT Enjeufaible · Contrôle faible	Situation tolérable à court terme. Attention : la dépendance s'installe progressivement.	Acceptez pour l'instant. Négociez une clause de sortie au prochain renouvellement.
SÉRÉNITÉ Enjeufaible · Contrôle élevé	Vous maîtrisez la situation. La faible criticité ne crée pas de risque majeur.	Déployez. Documentez les conditions qui vous permettent d'être dans cette zone.
DANGER Enjeuélevé · Contrôle faible	Zone des erreurs coûteuses. Enjeu élevé + incapacité à sortir = risque réel.	Renégociez le contrat ou changez de fournisseur avant de signer. Non négociable.
MAÎTRISE Enjeuélevé · Contrôle élevé	Vous avez fait le travail. La criticité est assumée, la dépendance est maîtrisée.	Maintenez cette logique sur tous vos projets à enjeu élevé.

4. MODE D'EMPLOI EN RÉUNION

1. **Nommezprécisément l'outil.**
Pas « déployer de l'IA » - mais « outil de transcription des consultations médicales » ou « assistant rédaction pour les appels d'offres ». La précision change le quadrant.

2. **Posez les deux questions à voix haute.**
Q1 : si ça tombe à 3h du matin, qui est impacté ? Est-ce qu'il y a une obligation légale ? Q2 : peut-on changer de fournisseur en 6 mois ? Y a-t-il une clause de sortie dans le contrat ?

3. **Lisez le quadrant. Agissez en conséquence.**
La zone DANGER n'est pas une nuance - c'est un signal d'alarme. Si personne dans la salle ne peut répondre à Q2, vous êtes probablement en DANGER.

À RETENIR Si vous ne pouvez pas répondre à Q2 avant de signer - vous n'avez pas décidé. Vous avez subi.

Un projet en zone DANGER coûte en moyenne 10× plus cher à corriger qu'à anticiper.

Cas d'usage - La clinique et la transcription IA

Application de la matrice sur un cas réel

CONTEXTE

Une clinique privée de 200 médecins veut déployer un outil d'IA qui transcrit automatiquement les consultations pour générer les comptes rendus médicaux. Le DSI présente la solution en réunion de direction : **un SaaS américain, modèle GPT-4, serveurs aux États-Unis, contrat annuel, données stockées chez le fournisseur.** Tout le monde est enthousiaste. Vous êtes dans la salle.

APPLICATION DE LA MATRICE

Q1 - ENJEU : élevé ↑

Pourquoi ?

Les données sont des **données de santé** - catégorie sensible par définition (RGPD). Le compte rendu médical est un **document légal** qui engage la responsabilité du médecin. Une erreur de transcription peut avoir des conséquences cliniques directes. L'hébergement doit être certifié **HDS** (Hébergeur de Données de Santé) en France.

Q2 - CONTRÔLE : faible ↓

Pourquoi ?

Serveurs aux États-Unis → **Cloud Act applicable** : le gouvernement américain peut accéder aux données sans notification. Pas de certification HDS. Contrat annuel sans clause de portabilité → **impossible de migrer les données** facilement. Modèle GPT-4 → **boîte noire**, pas d'audit possible du processus de transcription.

VERDICT

→ ZONE DANGER

Enjeu élevé (données de santé, responsabilité légale) + Contrôle faible (Cloud Act, pas HDS, pas de sortie)

CE QUE VOUS DITES EN RÉUNION

Trois questions à poser avant d'approuver 1. « Les serveurs sont en France ou en Europe avec certification HDS ? » - si non, c'est illégal pour des données de santé.

2. « Le contrat contient une clause de portabilité des données ? » - si non, on ne peut pas partir.

3. « Qui est responsable si la transcription contient une erreur médicale ? » - si la réponse est floue, on n'a pas le contrôle.

L'ALTERNATIVE - ZONE MAÎTRISE

Option A - SaaS EU certifié HDS

- Hébergement France (OVHcloud, Cegedim)
- Certification HDS obligatoire Clause de portabilité dans le contrat Données soumises au droit français

Option B - Solution on-premise

- Modèle open source déployé en local
- Données qui ne quittent jamais la clinique
- Aucune dépendance fournisseur externe
- Équipe interne ou prestataire EU maîtrisé

Ce cas illustre la règle la plus importante de la matrice :

L'enthousiasme collectif en réunion n'est pas une évaluation des risques.