LIVRE BLANC · PME ET ETI

Du numérique à l'IA, sans sauter la data

Guide pratique pour construire et gouverner sa stack data et IA

1. Le numérique
2. La data
3. L'IA

Datacculturation x Kilian B.

Édition de novembre 2026 · Guide neutre · Textes réglementaires et outils vérifiés en novembre 2026
Licence Creative Commons CC BY-NC-ND 4.0

Sommaire

Comment lire ce guide 3
Trois parcours de lecture, résumé exécutif

Partie 1. Pourquoi : les trois révolutions 5
Numérique, data, IA ; le saut de la deuxième ; erreurs classiques

Partie 2. Où en êtes-vous : la maturité numérique, data et IA 8
Modèle 0 à 4, auto-diagnostic, profils, prérequis, socle data minimal

Partie 3. Le modèle : une stack vivante 13
Neuf couches, règles d'architecture, choix structurants

Partie 4. La valeur : les cas d'usage 16
Priorisation, catalogue par fonction, indicateurs de valeur

Partie 5. L'architecture outillée 21
Types d'outils, exemples du marché, architectures PME et ETI

Partie 6. Profil technique 26
Flux, sécurité de l'IA, identité et autonomie des agents, évaluation, coûts

Partie 7. La donnée de bout en bout 34
Cycle de vie, conservation, qualité

Partie 8. Profil gouvernance 37
Organisation, RACI, RGPD et AI Act, charte, fournisseurs, incidents

Partie 9. Mise en œuvre 47
Diagnostic, trajectoires, feuille de route, budget, conduite du changement

Partie 10. Faire vivre la stack 55
Rituels, calendrier, tableau de bord de pilotage, gouvernance fédérée

Partie 11. Boîte à outils : matrices et gabarits 57
21 matrices et gabarits, de 11.1 à 11.21

Annexes 81
Glossaire, panorama des outils, hypothèses, sources

Du numérique à l'IA, sans sauter la data © 2026 by Datacculturation x Kilian B. is licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International.

Vous pouvez partager ce guide librement, à trois conditions : citer l'auteur, ne pas en faire un usage commercial, ne pas le modifier. Édition de novembre 2026, version 1.0.

OUVERTURE

Comment lire ce guide

Ce guide est écrit pour trois lecteurs : le dirigeant, l'équipe technique et la personne qui porte la gouvernance des données et du SI, en PME comme en ETI. Inutile de tout lire. Chacun a son parcours, et chaque partie s'ouvre sur un encadré « En bref » qui va droit à l'essentiel.

Direction et CODIR

Environ 30 minutes.

- Résumé exécutif
- Partie 1 : les trois révolutions
- Partie 2 : se situer (2.1 à 2.3)
- Partie 4 : la valeur
- Partie 9 : feuille de route et budget

Équipes techniques

Environ 35 minutes.

- Partie 2 : prérequis et socle minimal (2.4 à 2.6)
- Parties 3 et 5 : le modèle et les outils
- Partie 6 : profil technique
- Partie 7 : la donnée de bout en bout

Gouvernance donnée et SI

Environ 35 minutes.

- Partie 1 : le saut de la data (1.2)
- Partie 2 : la maturité
- Partie 7 : cycle de vie
- Partie 8 : profil gouvernance
- Partie 10 : faire vivre

Sur le bord droit des pages, une bande de couleur signale votre parcours, comme un intercalaire. En feuilletant, vous voyez tout de suite les pages qui vous concernent. La bande indique aussi la première et la dernière page de chaque parcours.

Direction : en haut du bord droit

Technique : au milieu

Gouvernance : en bas

Ce que vous trouverez dans ce guide

- **Un diagnostic**, pour savoir où vous en êtes en numérique, en data et en IA.
- **Un modèle d'architecture** qui parle de capacités et de règles. Pas une liste d'outils à acheter.
- **Une méthode** pour choisir vos cas d'usage, faire avancer data et IA en même temps, et tenir dans la durée.
- **Une boîte à outils** : matrices et gabarits à imprimer, puis à remplir en atelier.

Conventions

Trois couleurs vous suivront tout du long : **le rose pour le numérique**, **l'orange pour la data**, **le violet pour l'IA**. Quand un outil de la boîte à outils peut vous servir, un renvoi l'indique, comme ceci : *→ Matrice 11.1*.

Les outils cités servent d'exemples. Aucun n'est recommandé, et leurs offres bougent vite : vérifiez avant de signer quoi que ce soit.

OUVERTURE

Résumé exécutif

EN UNE PHRASE

L'IA ne remplace pas la data : elle la rend indispensable. Une entreprise peut commencer l'IA dès aujourd'hui, à condition de mener en parallèle la révolution qu'elle a peut-être sautée, celle de la donnée.

Le constat

Presque toutes les entreprises ont réussi leur première révolution, du papier au numérique. Beaucoup veulent maintenant sauter à la troisième, l'IA, sans avoir mené la deuxième : rassembler leurs données, s'accorder sur leur sens, les fiabiliser, les gouverner.

Le saut marche pour une partie des usages, ceux qui touchent aux documents et au travail de chacun. Il casse dès qu'on demande à l'IA de répondre sur des chiffres, de prévoir ou d'agir dans le SI. Elle s'appuie alors sur des données qui se contredisent. Le résultat ne peut pas être fiable.

Les chiffres vont dans le même sens. D'après Bpifrance Le Lab (2025), une PME ou une ETI qui analyse ses données a **2,5 fois** plus de chances d'utiliser l'IA. Et 43 % d'entre elles n'analysent pas leurs données pour piloter leur activité.

La réponse proposée

1. **Vous situer** sur trois axes notés de 0 à 4 : numérique, data, IA. → Partie 2
2. **Choisir des usages** à votre mesure, et lancer tout de suite ceux qui se passent de socle data. → Parties 2, 4
3. **Bâtir un socle data minimal** sur deux ou trois domaines, pas plus. → Partie 2.6
4. **Organiser une stack vivante**, aux outils remplaçables. → Parties 3 et 5
5. **Gouverner tout de suite** : propriétaires, registres, charte, conformité. → Partie 8

Quatre décisions pour le CODIR

Décision	Ce qu'elle engage
1. L'ambition et les premiers cas d'usage	Trois à cinq cas d'usage choisis pour leur valeur et leur faisabilité, avec un propriétaire nommé pour chacun.
2. Mener la data en parallèle de l'IA	Un socle data minimal financé et piloté comme un projet à part entière, pas comme une dépendance technique.
3. Les choix structurants	Niveau de souveraineté exigé, part de services managés et d'auto-hébergement, construire ou acheter.
4. La gouvernance	Un comité trimestriel, des propriétaires de données nommés, une charte d'usage de l'IA pour les salariés.

La trajectoire

Cadrer, **poser un socle minimal** sur deux ou trois domaines, **montrer de la valeur**. Ensuite seulement, **automatiser** sous validation humaine, puis **industrialiser**. Tous les six mois, un diagnostic dit si l'on avance.

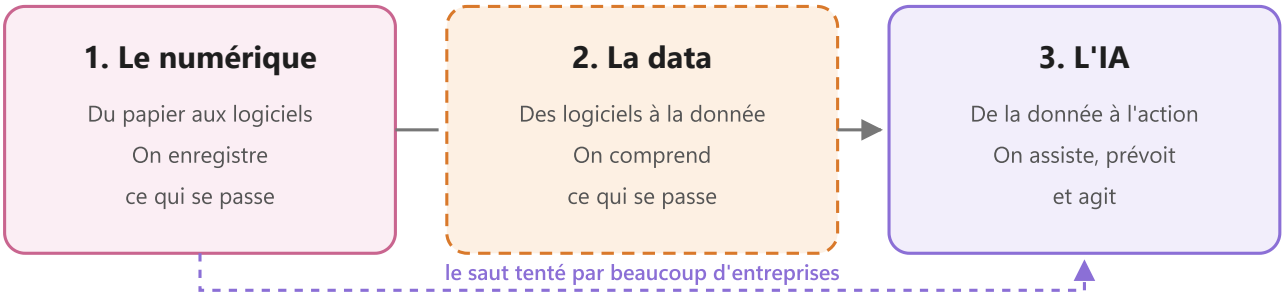
PARTIE 1

Pourquoi : les trois révolutions

EN BREF

- Numérique, data, IA : trois révolutions différentes, empilées l'une sur l'autre.
- Beaucoup d'entreprises essaient de passer du numérique à l'IA en sautant la data.
- Ça marche sur les documents. Pas sur les chiffres, ni dès que l'IA doit agir.
- Une stack organisée rapporte de la valeur, donne de la maîtrise et facilite la conformité.
- Cinq erreurs reviennent sans cesse. On peut toutes les éviter au cadrage.

1.1 Trois révolutions, trois changements de nature



Le numérique a remplacé le papier, les classeurs et les ressaisies par des logiciels : comptabilité, paie, caisse, ERP, CRM, messagerie. On a changé la façon d'*enregistrer* l'activité, et chaque logiciel est devenu la mémoire d'un service.

La data, c'est l'étape où ces mémoires sortent de leurs silos. On rassemble les données des différents logiciels dans un socle commun et on les nettoie. On décide une bonne fois ce que veut dire chaque indicateur : le chiffre d'affaires, une commande, un client actif. Et on nomme quelqu'un pour en répondre. Résultat, on *comprend* l'activité, et tout le monde regarde enfin les mêmes chiffres.

L'IA s'appuie sur les deux premières. Assistants et agents lisent les documents et les données, répondent, rédigent, prévoient, et finissent par déclencher des actions dans les logiciels. Cette fois, c'est la façon d'*agir* qui change.

Pourquoi la deuxième passe inaperçue. Elle n'apporte ni nouvel écran ni outil spectaculaire. On la remarque surtout quand elle manque : des réunions entières à réconcilier des chiffres, des fichiers Excel qui divergent, des indicateurs que personne ne sait définir.

1.2 Le saut de la deuxième révolution

Les assistants d'IA grand public ont ouvert un raccourci, du moins en apparence. En quelques secondes, n'importe quel salarié obtient un texte, une synthèse, une analyse. On a vite envie d'étendre ces usages à toute l'entreprise et de faire l'impasse sur le travail de fond sur les données.

Pourquoi le saut est tentant

- Les premiers résultats tombent tout de suite, alors qu'un projet data met des mois à produire quelque chose de visible.
- On peut se servir d'un outil d'IA sans passer par l'équipe informatique.
- La data a l'image d'un chantier technique. L'IA, celle d'un levier stratégique.

Ce que disent les études. Une PME ou une ETI qui analyse ses données a 2,5 fois plus de chances d'utiliser l'IA. Si elle est numérisée, c'est 5 fois plus (Bpifrance Le Lab, 2025). Gartner, de son côté, observe que les organisations qui réussissent avec l'IA investissent jusqu'à quatre fois plus dans leurs fondations (qualité des données, gouvernance, compétences) que celles qui échouent (2026).

Ce que le saut coûte

Symptôme	Cause
Des chiffres contradictoires	Chaque agent ou chaque utilisateur recalcule « le chiffre d'affaires » à sa façon, faute de définition commune.
Des réponses inventées	L'IA comble les trous quand elle n'a pas accès à une donnée fiable, et le fait avec assurance.
Des pilotes qui ne passent pas à l'échelle	Le pilote fonctionne sur un fichier préparé à la main ; la production exige des flux de données automatiques qui n'existent pas.
Des données qui sortent du cadre	Sans classification ni règles, des données confidentielles ou personnelles sont envoyées à des services externes.
Une dépendance subie	Les usages s'organisent autour d'un outil, et non autour de données maîtrisées : changer d'outil devient coûteux.

Attendre d'avoir fini la data ? Non. Une partie des usages d'IA peut démarrer dès demain (2.5). En revanche, **menez les deux de front**, et gardez l'IA à l'écart des chiffres et des actions tant que les données ne sont pas prêtes.

1.3 Le constat de terrain

Dans beaucoup d'entreprises, le point de départ ressemble à ce qui suit. Rien d'anormal là-dedans :

- **Des usages d'IA déjà là, mais invisibles.** Des salariés utilisent des assistants grand public sur leurs comptes personnels, sans règle ni suivi. C'est ce qu'on appelle la « shadow IA ».
- **Des données éparpillées** dans une dizaine de logiciels, que relient des exports faits à la main.
- **Des initiatives en ordre dispersé.** Un service a acheté un outil d'IA, un autre teste un agent dans son coin.
- **Une équipe informatique** sollicitée pour tout, mais rarement consultée sur l'IA.

1.4 Ce qu'apporte une stack data et IA organisée

Par « stack », on entend l'ensemble des briques techniques qui collectent, stockent, définissent, restituent et exploitent les données, IA comprise. Quand elle est organisée, on y gagne sur trois plans.

Bénéfice	Ce que cela change concrètement
Valeur	Les cas d'usage sont choisis pour ce qu'ils rapportent. Les réponses des agents reposent sur des chiffres partagés. Les pilotes réussis passent en production sans tout reconstruire.
Maîtrise	Chaque brique a un rôle clair et peut être remplacée. Les coûts sont suivis par cas d'usage. L'entreprise ne dépend pas d'un fournisseur unique.
Conformité	On sait quelles données vont où, qui y accède, combien de temps on les garde. Les obligations du RGPD et du règlement européen sur l'IA (AI Act) deviennent gérables.

1.5 Les cinq erreurs classiques

1. **Construire l'infrastructure avant d'avoir des cas d'usage.** On achète un entrepôt de données, une plateforme, des licences. Puis on cherche à quoi tout cela pourrait bien servir. On se retrouve avec une infrastructure sans client.
2. **Sauter la couche sémantique.** Si personne n'a fixé la définition des indicateurs, chaque tableau de bord et chaque agent calcule les chiffres à sa manière.
3. **Remettre la gouvernance à plus tard.** Les usages hors cadre s'installent avant les règles. Les faire rentrer dans le rang devient ensuite très difficile.
4. **Sous-estimer la maintenance.** Chaque brique demande du temps et des compétences. Dimensionnez la stack sur ce que votre équipe peut réellement faire tourner.
5. **Trancher la souveraineté trop tard.** L'endroit où doivent rester les données décide de l'hébergement et des modèles possibles. Revenir dessus après coup coûte cher.

> Toutes ces erreurs se règlent au cadrage. Pour cela, il faut d'abord savoir où l'on en est, et c'est ce que permet le diagnostic de la partie 2.

Partie 2. *Le constat est posé. Où en est votre entreprise ? Le diagnostic de maturité va vous le dire.*

PARTIE 2

Où en êtes-vous : la maturité numérique, data et IA

EN BREF

- On mesure la maturité sur trois axes séparés, notés de 0 à 4 : numérique, data, IA.
- Une demi-journée d'atelier et une grille notée suffisent pour situer l'entreprise.
- Le profil qui en sort dit quels usages d'IA sont réalistes dès maintenant.
- Une règle simple : sur les chiffres, l'IA ne doit pas devancer la data de plus d'un niveau.
- Pour débloquer la suite, un socle data minimal, taillé pour les usages prioritaires, suffit.

2.1 Le modèle de maturité

Il y a trois axes, un par révolution, chacun noté de **0** (rien) à **4** (avancé). Ils sont indépendants les uns des autres. On peut très bien avoir 3 en numérique, 1 en data et 2 en IA. C'est même le profil qui en apprend le plus.

Axe numérique : les processus et les outils

0 Papier	1 Outils isolés	2 Outils structurants	3 SI intégré	4 SI piloté et ouvert
Processus majoritairement papier ou par messagerie. Ressaisies fréquentes.	Un logiciel par service (comptabilité, paie, caisse), sans liens entre eux.	ERP ou CRM en place, processus clés dématérialisés, échanges par exports manuels.	Applications reliées par API ou connecteurs, identité unique, processus numériques de bout en bout.	Architecture documentée, flux automatisés, sécurité et hébergement maîtrisés.

Axe data : la donnée comme ressource

0 Données subies	1 Rapports manuels	2 Données centralisées	3 Données gouvernées	4 Donnée comme produit
Chiffres extraits à la main, au cas par cas. Chaque service a sa vérité.	Tableaux consolidés périodiquement dans un tableur. Définitions implicites.	Socle alimenté automatiquement sur quelques domaines. Définitions partielles.	Indicateurs définis et versionnés, propriétaires nommés, qualité mesurée.	Domaines couverts, données réutilisées par tous, décisions pilotées par la donnée.

Axe IA : les usages et leur cadre

0 Absente	1 Usages spontanés	2 Usages encadrés	3 Agents intégrés	4 IA industrialisée
Aucun usage connu, ou interdiction de principe.	Assistants grand public utilisés individuellement, sans cadre ni suivi.	Outil choisi, charte, formation, premiers assistants sur les documents.	Agents connectés aux données et au SI, cas d'usage au registre, évaluation.	Portefeuille piloté par la valeur, automatisations validées, conformité en routine.

Méfiez-vous du niveau 1 en IA. Il veut dire que des usages existent, pas que tout va bien. C'est souvent le niveau le plus risqué, parce que des données quittent l'entreprise sans que personne le sache.

DIRECTION

GOUVERNANCE

2.2 L'auto-diagnostic

Le diagnostic se fait en une demi-journée d'atelier. Autour de la table : un membre de la direction, un responsable informatique et deux ou trois personnes des métiers. Chaque axe est noté sur six critères. → *Matrice 11.1*

Numérique	Data	IA
N1. Processus dématérialisés	D1. Accès aux données	I1. Usages réels connus
N2. Couverture des applications métier	D2. Centralisation	I2. Cadre (outil, charte)
N3. Intégration entre outils	D3. Définition des indicateurs	I3. Compétences et formation
N4. Identité et accès	D4. Propriétaires des données	I4. Intégration aux données et au SI
N5. Hébergement et sécurité	D5. Qualité mesurée	I5. Gouvernance et conformité
N6. Compétences numériques	D6. Usage dans la décision	I6. Mesure de la valeur

Règles de calcul

1. Chaque critère reçoit une note de 0 à 4, à partir des descriptions de la matrice 11.1.
2. La note d'un axe, c'est la moyenne de ses six critères, **arrondie à l'entier inférieur**.
3. **Règle du maillon faible** : un seul critère à 0 et l'axe ne peut pas dépasser 2.
4. Si l'atelier n'arrive pas à se mettre d'accord, on garde la note la plus basse et on note le désaccord. Il cache souvent un vrai sujet.

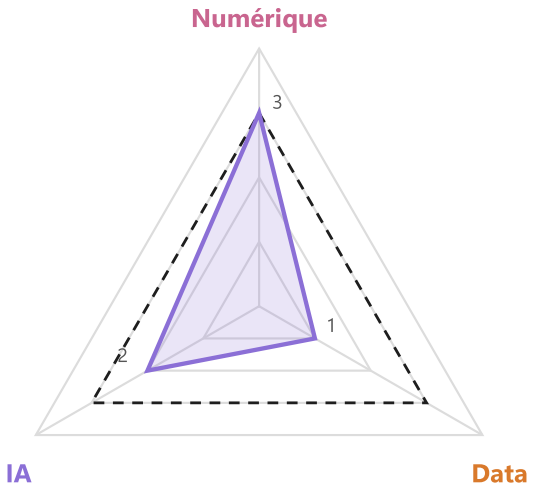
Le préalable : les conditions organisationnelles

Les trois axes ne disent pas si l'entreprise est organisée pour avancer. D'où quatre questions préalables, notées à part. Un **sponsor** est-il nommé à la direction ? Existe-t-il une **ambition** data et IA écrite ? Un **budget** dédié ? Du **temps** réservé pour les équipes ? Moins de deux oui, et la priorité devient le cadrage (9.1), pas la stack, quel que soit le radar.

> **Un conseil pour animer l'atelier.** Demandez toujours une preuve. « Montrez-moi où est écrite la définition du chiffre d'affaires. » Sur la data, un diagnostic purement déclaratif surestime presque toujours la maturité.

2.3 Lire son profil

On reporte les trois notes sur un radar. Regardez sa forme plutôt que sa taille.



Exemple : profil « la marche manquante » (numérique 3, data 1, IA 2). En pointillés, une cible à 18 mois (3, 3, 3).

Profils types

Profil	N · D · IA	Priorité
La marche manquante	3 · 1 · 2	Socle data minimal ; IA limitée aux documents
Le papier	1 · 0 · 1	Numériser d'abord ; cadrer l'IA spontanée
La data sans usage	3 · 3 · 0	Passer vite à l'IA, le socle est prêt
L'équilibre	2 · 2 · 2	Progresser sur les trois axes à la fois
L'avancé	4 · 3 · 3	Industrialiser, piloter par la valeur

Le profil **« la marche manquante »** est celui qui a motivé ce guide. Le numérique est solide, la data peu structurée, et les usages d'IA grandissent plus vite que le socle censé les porter. Le triangle penche côté IA et s'écrase côté data.

2.4 La règle des prérequis

Chaque famille d'usage d'IA demande un niveau minimal en numérique et en data. Le tableau sert à vérifier qu'un cas d'usage tient la route avant de le lancer. → *Matrice 11.3*

Famille d'usage d'IA	Numérique min.	Data min.	Si on saute les prérequis
Rédaction, synthèse, productivité individuelle	1	0	Risque surtout lié aux données saisies dans l'outil
Recherche dans les documents internes	2	1	Réponses fondées sur des documents périmés ou contradictoires
Assistance au service client (FAQ, procédures)	2	1	Réponses incohérentes d'un client à l'autre
Questions sur les chiffres (ventes, stock, marges)	2	3	Chiffres contradictoires, perte de confiance
Prévisions (ventes, stocks, trésorerie)	3	3	Prévisions construites sur un historique non fiable
Personnalisation marketing	3	3	Erreurs de ciblage, risque RGPD élevé
Agents qui agissent dans le SI (commandes, relances)	3	3	Actions erronées dans les logiciels de production

La règle que nous proposons. Pour les usages qui touchent aux chiffres ou qui agissent, visez en IA au plus un cran au-dessus de votre niveau data. Avec 1 en data, on peut viser 2 en IA. Pas 3.

2.5 L'IA sans socle data, et avec

Possible dès maintenant

- Rédaction, reformulation, traduction
- Synthèse de réunions et de documents
- Recherche dans la documentation interne, si elle est à jour
- Aide à la réponse client sur une FAQ validée
- Aide au code et à l'analyse ponctuelle de fichiers

Il faut quand même un outil choisi, une charte et des règles claires sur ce qu'on a le droit d'y saisir.

Exige d'abord un socle data

- Répondre sur les ventes, les marges, les stocks
- Produire des tableaux de bord automatiquement
- Prévoir la demande ou la trésorerie
- Personnaliser la relation client
- Déclencher des actions dans l'ERP ou le CRM

Il faut des données centralisées, des indicateurs définis et des propriétaires nommés.

Commencer par la colonne de gauche n'a rien d'un pis-aller. Ces usages rapportent vite, forment les équipes et font remonter les besoins en données qui orienteront le socle.

2.6 Le socle data minimal viable

Le socle data minimal, c'est le plus petit investissement qui débloque vos usages d'IA prioritaires. Il n'a pas vocation à couvrir toute l'entreprise.

Composant	Périmètre minimal
Domaines couverts	Deux ou trois, choisis par les cas d'usage prioritaires (par exemple ventes, stock, service client).
Collecte	Extraction automatique et régulière des logiciels sources concernés, sans ressaisie.
Stockage	Un entrepôt de données managé, organisé en zones (brut, nettoyé, métier).
Définitions	Les dix à vingt indicateurs qui comptent, définis une fois, versionnés, avec un responsable chacun.
Propriété	Un propriétaire métier nommé pour chaque domaine.
Qualité	Quelques tests automatiques (doublons, valeurs manquantes, fraîcheur) et une alerte en cas d'échec.
Restitution	Un premier tableau de bord partagé qui lit les définitions communes.

Repères PME

- Services managés uniquement
- Deux domaines
- Un responsable interne à temps partiel, appuyé par un prestataire

Repères ETI

- Socle managé, éventuellement mixte
- Trois domaines, puis extension
- Une petite équipe data dédiée

Les ordres de grandeur de budget et de délais sont en partie 9.

2.7 Mesurer la progression

Le diagnostic n'a rien d'un audit qu'on range dans un tiroir. On le refait **tous les six mois**, avec la même grille et, si possible, les mêmes personnes. Trois choses à suivre :

- **L'évolution du radar.** Le triangle doit d'abord se rééquilibrer, puis grandir.
- **Les critères à 0.** Ils plafonnent tout un axe, alors on s'en occupe en premier.
- **L'écart entre data et IA.** Au-delà d'un niveau, les usages d'IA sur les chiffres deviennent risqués.

> Le radar fait partie du tableau de bord présenté au comité (partie 10), avec la valeur, la santé de la stack et les risques.

Partie 3. *On sait d'où l'on part. Reste à voir vers quoi l'on va : le modèle d'une stack vivante.*

PARTIE 3

Le modèle : une stack vivante

EN BREF

- Une stack vivante se reconnaît à ses capacités et à ses règles. Les outils, eux, passent.
- Neuf couches plus un socle transversal, chacune avec son contrat.
- La donnée suit un seul chemin, et les agents comme les tableaux de bord la lisent au même endroit.
- Cinq règles d'architecture rendent chaque outil remplaçable.
- Trois choix structurants sont à trancher dès le début.

3.1 Le principe directeur

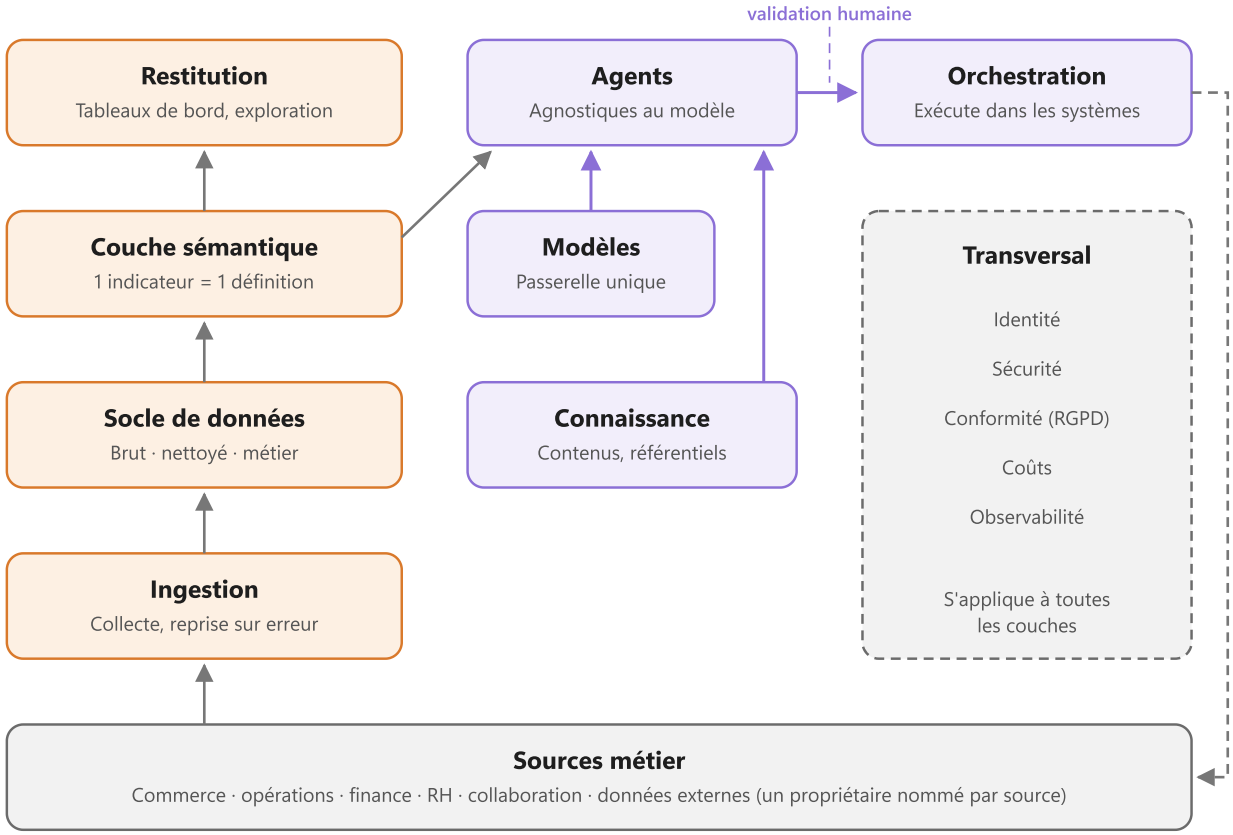
Une stack vivante se définit par ses **capacités** et ses **contrats**, bien plus que par ses outils. Chaque outil occupe une case, et doit pouvoir en sortir. Le test est simple : si l'on ne peut pas retirer un outil sans tout casser, la stack est figée.

3.2 Le modèle en couches

Couche	Rôle	Contrat à respecter
1. Sources	Systèmes métier (vente, produit, stock, support, RH, finance)	Chaque source a un propriétaire métier nommé
2. Ingestion	Collecte régulière vers le socle	Reprise sur erreur, traçabilité, aucune logique métier
3. Socle de données	Stockage central en trois zones : brut, nettoyé, métier	Brut jamais modifié, accès par zone
4. Couche sémantique	Définition unique et versionnée des indicateurs	Un indicateur = une définition = un responsable
5. Restitution	Tableaux de bord et exploration	Lit uniquement la couche sémantique
6. Connaissance	Contenus et référentiels éditoriaux	Source de vérité unique, exposée par API
7. Agents	Assistants et agents, agnostiques au modèle, reliés aux outils par des connecteurs standard (MCP)	Accès hérité des droits de l'utilisateur ; connecteurs approuvés uniquement
8. Modèles	Accès aux modèles via une passerelle unique	Routage par cas d'usage, changement sans refonte ; un seul chemin, y compris pour les appels d'outils
9. Orchestration	Enchaînement des actions entre systèmes	Validation humaine sur toute action irréversible
Transversal	Identité, sécurité, conformité, coûts, observabilité	Applicable à toutes les couches dès le départ

3.3 La vue d'ensemble

Le schéma se lit de bas en haut. Les données montent des sources jusqu'aux usages.



Orange : données · **violet** : IA et automatisation · **gris** : sources et transversal · pointillés : optionnel ou transversal.

Trois choix de structure

1. **La donnée suit un seul chemin** : sources, ingestion, socle, couche sémantique. Agents et tableaux de bord lisent la couche sémantique, ou les tables métier qui la portent. Jamais le socle brut. C'est ce qui évite d'avoir deux chiffres d'affaires différents dans la même réunion.
2. **La connaissance court en parallèle du socle.** Elle alimente directement les agents. Une fiche produit ou une procédure ne vit pas au même rythme qu'une table de ventes.
3. **L'orchestration se tient à côté des agents, pas au-dessus.** L'agent propose, l'orchestration exécute. La validation humaine se place entre les deux.

3.4 Les couches et les trois révolutions

Chaque couche dépend surtout de l'une des trois révolutions de la partie 1. Le tableau fait le lien avec votre diagnostic : un axe faible vous montre les couches à renforcer.

Révolution	Couches concernées	Signe qu'elle manque
Numérique	1. Sources ; identité et sécurité (transversal)	Ressaisies, comptes partagés, logiciels non reliés
Data	2. Ingestion ; 3. Socle ; 4. Couche sémantique ; 5. Restitution ; 6. Connaissance	Chiffres contradictoires, consolidations manuelles, documents périmés
IA	7. Agents ; 8. Modèles ; 9. Orchestration	Usages spontanés sans cadre, outils isolés

Sur neuf couches, cinq relèvent de la data. On retrouve dans l'architecture ce que disait le constat de départ : même quand on vise l'IA, c'est la deuxième révolution qui porte l'essentiel de la stack.

3.5 Les cinq règles d'architecture

1. **Traiter les données comme un produit.** Chaque jeu de données a un propriétaire, une définition et un niveau de qualité annoncé.
2. **Séparer les rôles** : collecter, transformer, définir, afficher, automatiser. L'outil qui prétend tout faire devient le point qui fait tout tomber.
3. **Pas de droits propres pour les agents.** Ils héritent de ceux de la personne qui les utilise, point.
4. **Prévoir la sortie.** Chaque choix d'outil documente comment on le quitte : export des données, des configurations, des consignes données aux agents. Les standards ouverts aident beaucoup, notamment Apache Iceberg, Open Semantic Interchange et MCP.
5. **Rester sobre.** On n'ajoute une capacité que si un cas d'usage prioritaire la réclame.

3.6 Les choix structurants

Trois décisions pèsent sur tout le reste. Elles se prennent au cadrage, en CODIR.

Choix	Question à trancher	Repère par défaut
Souveraineté	Les données peuvent-elles être traitées hors de l'Union européenne, ou par des fournisseurs soumis à des lois extraterritoriales ?	Hébergement en UE dans tous les cas ; option souveraine si contrainte client, sectorielle ou stratégique (9.6, scénario C). En France, la qualification SecNumCloud de l'ANSSI signale les offres de cloud de confiance
Managé ou auto-hébergé	L'équipe a-t-elle la capacité d'exploiter des serveurs, des mises à jour, des sauvegardes ?	PME : tout managé. ETI : managé, auto-hébergement ciblé là où il apporte un vrai gain
Construire ou acheter	L'usage est-il différenciant pour l'entreprise, ou standard ?	Acheter le standard (assistant, BI, ingestion) ; construire seulement ce qui fait la différence

Ces choix ne figent pas les outils. Ils posent le cadre dans lequel on les choisira, puis on les remplacera. → *Matrice 11.6*

Partie 4. *Le modèle liste des capacités. Ce sont les cas d'usage qui disent lesquelles construire, et dans quel ordre.*

PARTIE 4

La valeur : les cas d'usage

EN BREF

- On juge un cas d'usage sur trois critères : ce qu'il rapporte, s'il est faisable, ce qu'il risque.
- La faisabilité dépend directement de la maturité mesurée en partie 2.
- Le premier portefeuille compte trois à cinq cas, dont au moins un gain rapide qui se passe de socle data.
- La valeur se mesure avant, pendant et après le pilote, par rapport à une situation de départ.
- Chaque cas franchit cinq étapes aux critères connus d'avance. S'il est à faible risque, il peut prendre la voie rapide.

4.1 Identifier et prioriser

Trouver les cas d'usage

Les bons cas d'usage sortent rarement d'une démonstration technologique. Ils sortent de questions toutes simples posées aux équipes :

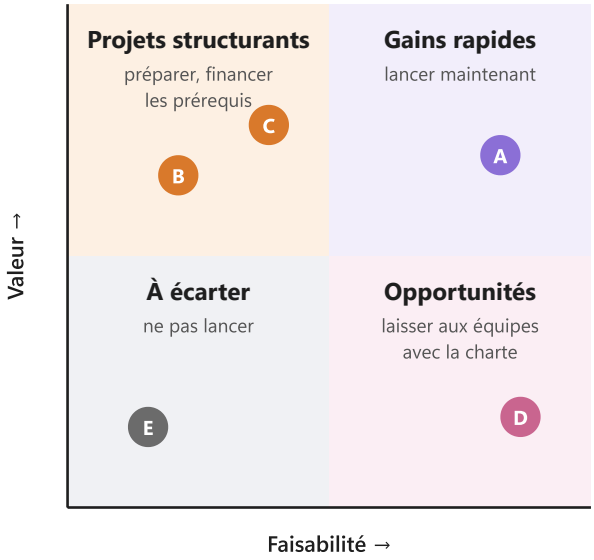
- Quelle tâche répétitive vous prend le plus de temps chaque semaine ?
- Quelle information cherchez-vous souvent sans la trouver ?
- Quelle décision prenez-vous sans les chiffres dont vous auriez besoin ?
- Quelle erreur coûte cher et revient régulièrement ?

Chaque idée retenue tient sur une fiche cas d'usage. → *Gabarit 11.11*

Noter chaque cas sur trois critères

Critère	Ce qu'on évalue	Échelle
Valeur	Temps gagné, revenu supplémentaire, coût évité, qualité, risque réduit. Nombre de personnes concernées.	1 (marginale) à 5 (forte, mesurable)
Faisabilité	Écart de maturité (matrice 11.3), disponibilité des données, complexité d'intégration, sponsor métier disponible.	1 (prérequis absents) à 5 (réalisable tout de suite)
Risque	Classe des données utilisées, conséquence d'une erreur, niveau d'autonomie de l'agent (6.4), catégorie au sens de l'AI Act.	Faible, moyen ou élevé

Valeur et faisabilité placent le cas dans une matrice. Le risque, lui, ne se rattrape pas avec un bon score. S'il est élevé, il faut l'avis du référent conformité et une validation humaine à chaque fois. → *Matrice 11.2*



A : synthèse des comptes rendus. B : prévision des stocks. C : questions sur les ventes. D : reformulation de courriels. E : agent client autonome sans base validée.

Les quatre zones

- **Gains rapides** : beaucoup de valeur, faisables tout de suite. Ce sont eux qui prouvent que la démarche fonctionne.
- **Projets structurants** : beaucoup de valeur, mais des prérequis manquent. Ce sont eux qui justifient le socle data minimal.
- **Opportunités** : faciles, peu stratégiques. Les équipes peuvent s'en emparer seules, dans le respect de la charte.
- **À écarter** pour l'instant. On les reverra quand la maturité aura progressé.

Composer le premier portefeuille. Trois à cinq cas d'usage. Au moins **un gain rapide** qui n'attend pas le socle data, et au moins **un projet structurant** dont les besoins dessinent le périmètre de ce socle. Avec seulement des gains rapides, on ne prépare rien. Avec seulement des projets structurants, on ne montre rien avant longtemps.

Pièges de la priorisation

- **Le cas d'usage du dirigeant.** Il passe en tête sans être noté. Notez-le comme les autres.
- **La démonstration du fournisseur.** Elle impressionne sur des données préparées pour l'occasion, et ne dit rien de ce qui marchera chez vous.
- **La valeur qu'on ne chiffre pas.** « On va gagner du temps », d'accord. Combien d'heures, pour combien de personnes, et pour faire quoi à la place ?
- **Le risque qu'on oublie.** Un cas simple et utile peut toucher à des données personnelles, ou tomber dans une catégorie sensible de l'AI Act.

4.2 Catalogue de cas d'usage types

Ce catalogue est un point de départ pour vos ateliers. Pour chaque cas, il donne la famille d'usage (voir 2.4), le niveau data minimal et une difficulté indicative. À vous de noter ensuite vos propres cas.

Fonction	Cas d'usage	Famille	Data min.	Difficulté
Ventes	Réponse aux appels d'offres à partir de la base documentaire	Documents internes	1	Faible
	Préparation d'un rendez-vous client (historique, échanges, commandes)	Documents et chiffres	2	Moyenne
	Questions en langage naturel sur les ventes et les marges	Questions sur les chiffres	3	Moyenne
Marketing	Déclinaison de contenus par canal et par cible	Productivité	0	Faible
	Analyse des avis et verbatims clients	Documents internes	1	Moyenne
	Segmentation et personnalisation des campagnes	Personnalisation	3	Élevée
Service client	Suggestion de réponses aux conseillers à partir de la FAQ	Assistance client	1	Faible
	Tri, résumé et routage des demandes entrantes	Assistance client	1	Moyenne
	Agent en libre-service pour les clients	Agent qui agit	3	Élevée
Opérations	Assistant sur les procédures qualité et sécurité	Documents internes	1	Faible
	Alerte sur les risques de rupture	Questions sur les chiffres	3	Moyenne
	Prévision des stocks et de la demande	Prévisions	3	Élevée
Achats	Comparaison d'offres fournisseurs	Documents internes	1	Faible
	Analyse des clauses de contrats fournisseurs	Documents internes	1	Moyenne
Finance	Commentaire des écarts budgétaires	Questions sur les chiffres	3	Moyenne
	Contrôle et rapprochement des factures	Agent qui agit	3	Moyenne
	Prévision de trésorerie	Prévisions	3	Élevée
RH	Rédaction d'offres d'emploi	Productivité	0	Faible
	Assistant aux questions des salariés (accords, procédures)	Documents internes	1	Moyenne
	Tri ou évaluation de candidatures **(catégorie sensible)**	Agent qui agit	3	Élevée
Direction	Synthèse de veille sectorielle et réglementaire	Productivité	0	Faible
	Tableau de bord commenté pour le CODIR	Questions sur les chiffres	3	Moyenne
Informatique	Aide au code et à la documentation	Productivité	0	Faible
	Support utilisateur de premier niveau	Assistance client	1	Moyenne

Catégorie sensible. L'AI Act classe à haut risque les systèmes d'IA utilisés pour recruter ou évaluer des personnes (annexe III, point 4, emploi et gestion des travailleurs). Les obligations renforcées s'appliquent à partir du 2 décembre 2027. Voir partie 8.

4.3 Mesurer la valeur

Il existe deux familles d'indicateurs, et il ne faut pas les mélanger. Ceux de **santé** disent si la stack tourne (fraîcheur des données, taux d'échec des flux). Ceux de **valeur** disent si elle sert à quelque chose. On parle ici des seconds.

Type de valeur	Indicateur	Comment le mesurer
Temps	Heures gagnées par mois sur la tâche	Chronométrage avant et pendant le pilote, sur un échantillon
Qualité	Taux d'erreur, délai de réponse, taux de reprise	Contrôle d'échantillons, données du logiciel métier
Revenu	Taux de transformation, panier moyen, taux de réponse	Comparaison avec un groupe témoin si possible
Coût évité	Prestations, pénalités, stocks dormants évités	Données financières avant et après
Risque	Incidents, non-conformités, litiges	Registre des incidents
Adoption	Utilisateurs actifs par semaine, taux de réutilisation	Journaux d'usage de l'outil

La méthode en trois temps

1. **Avant le pilote**, on mesure la situation de départ. Sans elle, impossible de prouver le moindre gain.
2. **Pendant le pilote**, on mesure les mêmes indicateurs, sur les mêmes personnes, de la même façon.
3. **Une fois en production**, on suit l'adoption et la valeur chaque trimestre, en revue du comité.

Le calcul du retour sur investissement

Retour sur investissement = (gains annuels − coûts annuels) ÷ coûts annuels

Côté coûts, comptez les licences, la consommation des modèles, l'intégration, le temps des équipes internes, l'exploitation et la maintenance. Le détail est en partie 9.

Du temps gagné à la valeur. Une heure gagnée ne vaut de l'argent que si on la réemploie : davantage de clients servis, moins d'heures supplémentaires, une tâche plus utile. Dites toujours à quoi servira le temps libéré.

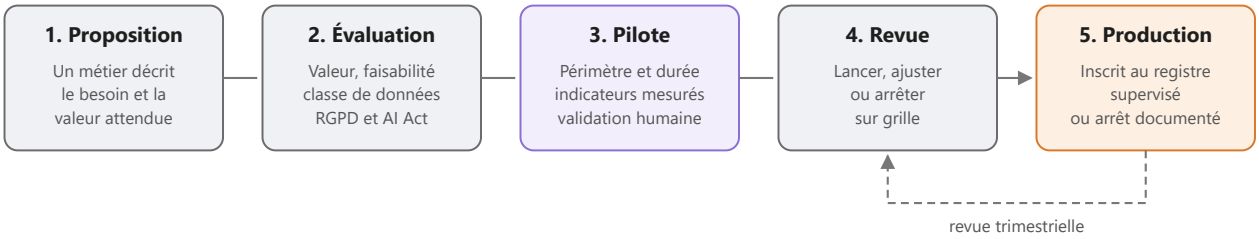
Ce qui doit déclencher l'arrêt d'un cas d'usage

- L'adoption reste faible une fois passée la période de prise en main.
- La valeur mesurée reste très en dessous de l'estimation, et on ne voit pas comment l'améliorer.
- Le cas coûte plus cher à faire tourner qu'il ne rapporte.
- Un nouveau risque apparaît, qu'on ne sait pas maîtriser.

Arrêter un cas d'usage n'a rien d'honteux. Au contraire, cela montre que la gouvernance joue son rôle. On note l'arrêt au registre, avec ce qu'on en a appris.

4.4 Le cycle de vie d'un cas d'usage

Chaque cas d'usage suit cinq étapes. On passe de l'une à l'autre sur des critères connus d'avance.



Étape	Critère pour passer à l'étape suivante	Qui décide
1. Proposition	Fiche cas d'usage complète, avec un propriétaire nommé et une valeur estimée chiffrée.	Propriétaire du cas d'usage
2. Évaluation	Notes de valeur et de faisabilité, prérequis vérifiés (11.3), classe de données identifiée, avis du référent conformité si le risque est élevé.	Comité, sur proposition
3. Pilote	Durée limitée (souvent 6 à 12 semaines), situation de référence mesurée, indicateurs suivis, validation humaine sur toute action.	Propriétaire du cas d'usage
4. Revue	Valeur mesurée comparée à la valeur estimée, adoption, coût de fonctionnement prévisionnel, risques constatés.	Comité
5. Production	Inscription au registre, propriétaire nommé, supervision en place, plan d'arrêt connu. Revue chaque trimestre.	Comité, puis propriétaire

La voie rapide. Faire attendre trois mois un cas sans enjeu, c'est le meilleur moyen de faire revenir la shadow IA. Un cas peut donc être validé au fil de l'eau par son propriétaire et le référent conformité, puis inscrit au registre, à cinq conditions. Le risque est faible. Seules des données publiques ou internes sont en jeu, aucune donnée personnelle. L'agent n'engage aucune action irréversible. Et l'outil est déjà approuvé. Le comité l'apprend à la revue suivante. S'il manque une seule condition, on repasse par la voie normale.

Ce cycle s'appuie sur l'organisation décrite en partie 8 : comité, rôles, registres.

Partie 5. *Les cas d'usage retenus disent quelles cases du modèle occuper. Il reste à choisir les outils pour les remplir.*

PARTIE 5

L'architecture outillée

EN BREF

- À chaque couche du modèle correspond un type d'outil, et le marché propose plusieurs candidats.
- Les pastilles en gras indiquent un point de départ minimal, qui n'engage à aucun achat.
- Deux alternatives d'une même case ne s'additionnent pas : on en choisit une.

5.1 Types d'outils et exemples du marché

Les usages sont en haut, les sources en bas. La liste n'est pas exhaustive. Nous l'avons vérifiée en novembre 2026, mais les offres, les prix et les positionnements bougent vite (voir A.2).

1 Restitution et BI

Tableaux de bord et exploration, lisent uniquement la couche sémantique

Data Studio · Metabase · Lightdash · Power BI

2 Plateforme agentique

Assistants et agents agnostiques au modèle, droits hérités de l'utilisateur

Dust · Copilot Studio · Langdock

Connecteurs vers les outils et les données

Serveurs MCP · A2A (entre agents)

3 Orchestration

Enchaîne les actions entre systèmes, validation humaine sur l'irréversible

Automatisations métier

n8n · Make · Zapier

Pipelines de données (optionnel au démarrage)

Dagster · Airflow · Kestra

4 Modèles et passerelle

Accès unique aux modèles, routage par cas d'usage

Modèles

Claude · **GPT** · **Mistral** · Gemini

Passerelle

LiteLLM · OpenRouter

5 Recherche sémantique optionnel

Index vectoriel pour retrouver les contenus pertinents

pgvector · Qdrant · Weaviate

6 Connaissance et référentiels

Fiches produit, FAQ, documentation, exposées par API aux agents

Strapi · Notion · Google Drive

TECHNIQUE

7 Transformation et couche sémantique

Nettoyage versionné et testé, définition unique des indicateurs

Transformation

dbt SQLMesh

Couche sémantique

dbt Semantic Layer Cube Lightdash

8 Socle de données

Entrepôt central en trois zones : brut, nettoyé, métier

BigQuery Snowflake Postgres / ClickHouse (souverain)

9 Ingestion (ELT)

Collecte régulière, reprise sur erreur, aucune logique métier

Airbyte Fivetran dlt

10 Sources métier

Catégories types, à remplacer par l'existant réel de l'entreprise

Commerce et clients

ERP CRM E-commerce Point de vente Marketing automation Service client

Opérations

WMS / logistique Production / MES Achats PLM GMAO Gestion de projet

Fonctions support

Finance / comptabilité SIRH / paie Juridique / contrats Support IT / ITSM

Collaboration

Suite bureautique Messagerie GED / intranet Wiki interne

Données externes

Open data Données de marché Partenaires / EDI IoT / capteurs Réseaux sociaux

T Transversal

S'applique à toutes les couches dès le départ

Identité et accès

SSO Google Workspace Okta

Observabilité IA et qualité des données

Langfuse Elementary

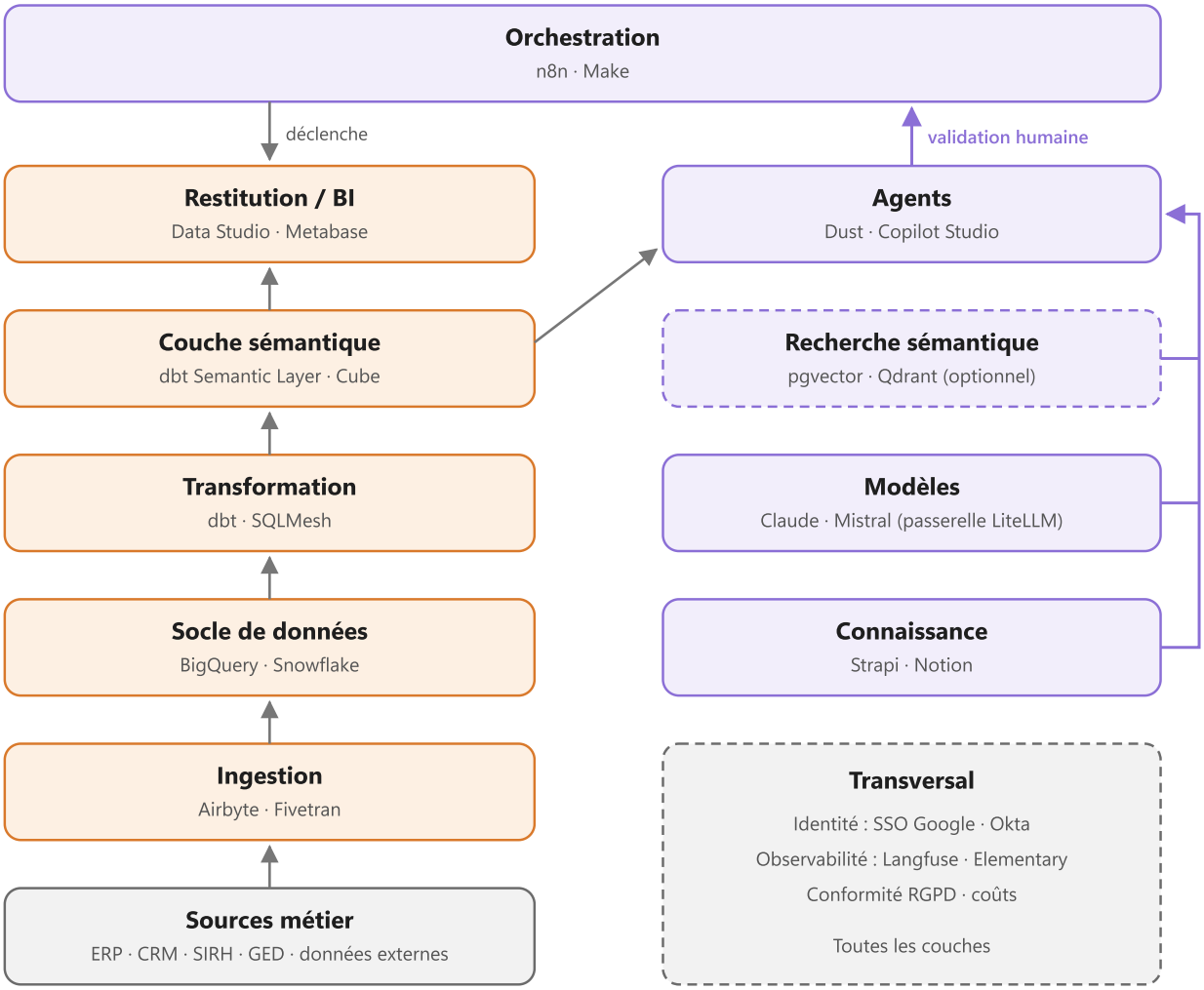
Conformité et coûts

Registre RGPD Classification des données Journal d'usage

- La couche 10 décrit des catégories types. Remplacez-les par ce que vous avez réellement.
- Pour démarrer au plus juste : socle et couche sémantique sur deux ou trois domaines, puis les agents. Les couches 3 (pipelines) et 5 attendront qu'un cas d'usage les réclame.
- Certains doublons sont voulus, comme Lightdash en BI et en couche sémantique, ou Dust et Copilot Studio. Ce sont des alternatives pour une même case.

5.2 La vue détaillée en schéma

À gauche, la chaîne de données, à lire de bas en haut. À droite, l'IA. Les agents lisent la couche sémantique (la flèche en diagonale) et s'appuient sur la connaissance et les modèles (la flèche qui remonte par la marge droite). En haut, l'orchestration déclenche et relie les deux colonnes. Le transversal vaut pour toutes les couches. On a gardé deux outils par case.



Orange : données · **violet** : IA et automatisation · **gris** : sources et transversal · pointillés : optionnel ou transversal.

5.3 Choisir un outil

On choisit un outil pour une case précise du modèle et pour des cas d'usage précis. Jamais sur la foi d'une démonstration. Comptez cinq temps.

1. **Partir du besoin** : quelle case, quels cas d'usage la réclament, quelles contraintes (données, volumes, souveraineté).
2. **Présélectionner trois candidats**, pas un de plus. Au-delà, on compare en surface.
3. **Noter sur une grille pondérée**, arrêtée avant de rencontrer le moindre fournisseur.
4. **Essayer sur vos données**, pendant deux à quatre semaines, sur un vrai cas d'usage et avec vos propres sources.
5. **Décider, puis documenter** le choix au registre des composants, plan de sortie compris.

Les critères et leur poids indicatif

Critère	Ce qu'on vérifie	Poids
Adéquation au besoin	Couvre les cas d'usage prévus, sans développement lourd	20
Intégration	Connecteurs vers vos sources, API ouvertes, identité unique (SSO)	15
Sécurité et conformité	Localisation, contrat de sous-traitance, gestion des droits, journalisation	15
Coût total sur trois ans	Licences, consommation, intégration, exploitation, évolution des prix	15
Réversibilité	Export des données et des configurations, formats ouverts	10
Exploitabilité	Compétences requises, part de service managé, documentation	10
Solidité du fournisseur	Pérennité, support en français, feuille de route, références comparables	10
Ouverture	Pour les briques d'IA : choix et changement de modèle possibles, connecteurs standard (MCP)	5

Ce qui compte le plus selon la case

Case	Critères à surpondérer
Socle de données	Coût à votre volume, localisation, compatibilité avec les outils de transformation
Plateforme d'agents	Gestion des droits par espace, connecteurs, indépendance aux modèles, journalisation
BI et restitution	Lecture de la couche sémantique, facilité pour les métiers, coût par lecteur
Ingestion	Connecteurs vers vos sources réelles, reprise sur erreur, coût au volume

→ *Matrice 11.6*

5.4 Trois architectures types

Ces trois architectures correspondent aux scénarios de budget de la partie 9.6. Elles décrivent des types d'outils ; pour des noms, voyez la partie 5.1.

Couche	A. PME, tout managé	B. ETI, mixte	C. Option souveraine
Ingestion	Service d'ingestion en ligne	Service en ligne, connecteurs maison ciblés	Outil open source auto-hébergé
Socle	Entrepôt cloud managé, région UE	Entrepôt cloud managé, région UE, tables en format ouvert (Iceberg) si possible	Base analytique chez un hébergeur européen, format de tables ouvert
Transformation et sémantique	Modèles de transformation simples, métriques dans l'outil de BI	Outil de transformation versionné, couche sémantique dédiée	Comme B, auto-hébergé
Restitution	BI en ligne gratuite ou d'entrée de gamme	BI gouvernée	BI open source auto-hébergée
Connaissance	Espace documentaire existant, nettoyé	Référentiel éditorial avec API	Référentiel open source auto-hébergé
Recherche sémantique	Incluse dans la plateforme d'agents	Index vectoriel dédié si besoin	Index vectoriel auto-hébergé
Agents	Plateforme d'agents en ligne	Plateforme d'agents en ligne, gouvernée par espaces	Plateforme européenne ou auto-hébergée
Connecteurs d'agents	Connecteurs MCP fournis par la plateforme	Serveurs MCP approuvés, droits minimaux par outil	Serveurs MCP auto-hébergés
Modèles	Via la plateforme d'agents	Via la plateforme, passerelle pour les appels directs	Modèles européens ou ouverts, hébergés en UE
Orchestration	Outil d'automatisation en ligne	Orchestrateur auto-hébergé	Orchestrateur auto-hébergé
Transversal	SSO de la suite bureautique	SSO, coffre à secrets, observabilité, CI/CD	Comme B, chez un hébergeur européen
Briques à exploiter	1 à 2	4 à 6	8 et plus

Lisez d'abord la dernière ligne. Chaque brique que vous hébergez vous-même réclame des mises à jour, des sauvegardes, de la surveillance et des compétences. Choisissez l'architecture en fonction de ce que votre équipe saura vraiment faire tourner.

Faire évoluer l'architecture

- On peut glisser de A vers B progressivement, couche par couche, au rythme des cas d'usage.
- Passer à C après coup coûte plus cher. La question de la souveraineté se règle au cadrage (3.6).
- Les règles d'architecture (3.5), surtout la réversibilité, permettent ces évolutions sans tout reconstruire.

Partie 6. *Les trois parties qui suivent changent d'angle. On regarde la même architecture avec les yeux de l'équipe technique, puis de la donnée, puis de la gouvernance.*

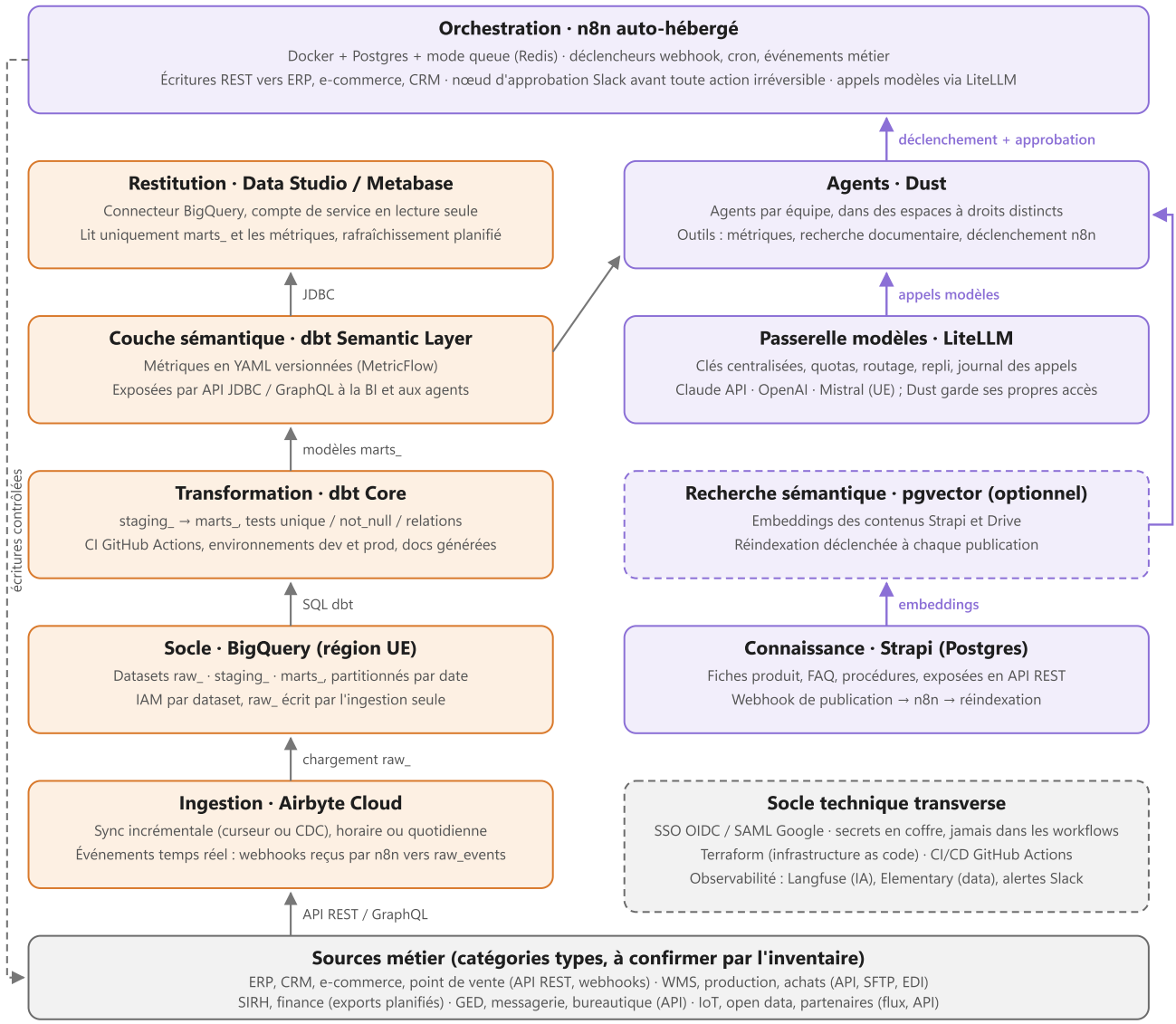
PARTIE 6

Profil technique

EN BREF

- On reprend la même architecture, cette fois du point de vue de ceux qui la construisent et la font tourner.
- Pour chaque brique : connexions, données, déploiement, surveillance.
- S'il ne faut pas reporter une chose, c'est la sécurité de l'IA (6.4), avec l'identité et l'autonomie des agents.

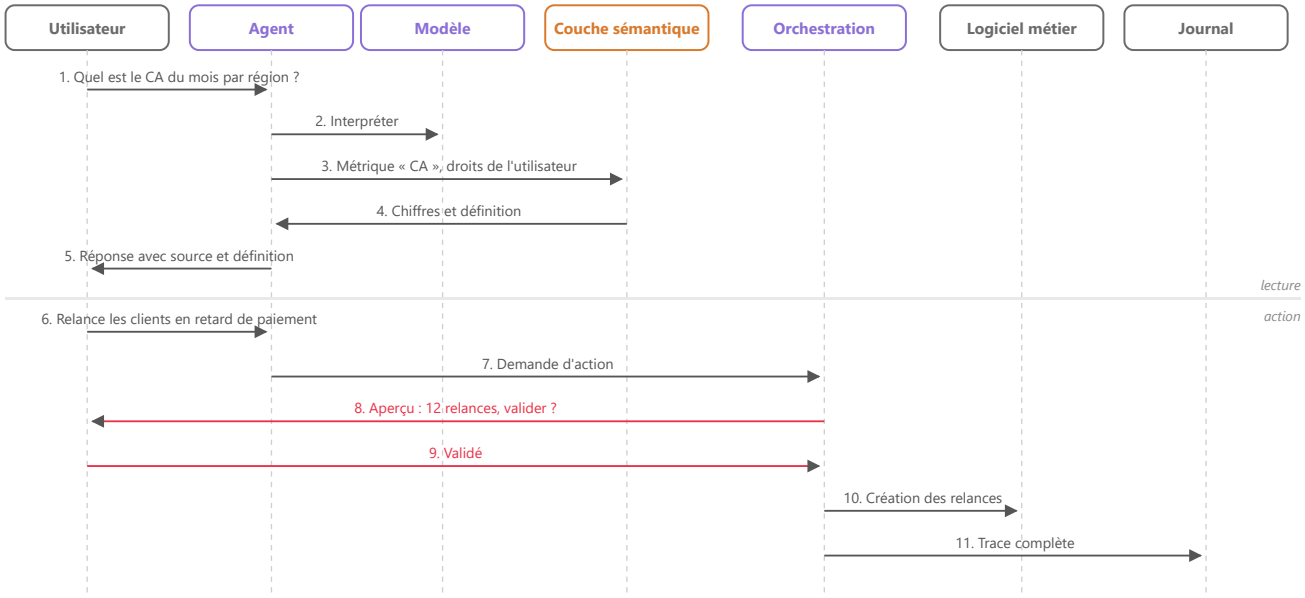
6.1 Flux, protocoles et exploitation



- Visez un seul chemin vers les modèles et les outils : la passerelle, qui porte aussi de plus en plus les appels d'outils MCP. Si la plateforme d'agents garde ses propres accès, notez l'exception au registre des composants.
- Les agents ne touchent jamais raw_. Ils lisent les métriques ou marts_ avec un compte de service en lecture seule, filtré selon l'espace.

6.2 Le flux d'une demande type

Prenons une demande en deux temps : d'abord une question sur les chiffres, ensuite une action. Le schéma montre les couches traversées et l'endroit où se placent les contrôles. En rouge, la validation humaine.



Étape	Contrôle	Ce qu'il empêche
1	Connexion par l'identité unique de l'entreprise ; l'agent connaît l'utilisateur et son espace	Accès anonyme, usurpation
2	Appel au modèle via la passerelle : quotas, journal, pas de données au-delà du nécessaire	Dérive de coûts, fuite vers le fournisseur
3 et 4	L'agent interroge la couche sémantique, jamais le brut, avec les droits de l'utilisateur	Chiffres contradictoires, fuite de données
5	La réponse cite la métrique, sa définition et la date des données	Réponse invérifiable
7 à 9	L'action passe par l'orchestration, qui présente un aperçu et attend une validation	Action erronée ou issue d'une injection
Variante	Si l'agent appelle directement un outil par un connecteur MCP, les mêmes règles s'appliquent : droits de l'utilisateur, connecteur approuvé, validation humaine avant toute écriture	Contournement de l'orchestration
10	Écriture par un compte de service limité à cette action, avec plafond	Modification massive non voulue
11	Trace de la demande, de la réponse, de la validation et de l'action	Incident impossible à analyser

6.3 Les données de référence

Le même client existe dans l'ERP, le CRM et l'outil d'emailing, avec trois orthographes et trois identifiants. Le même produit porte une référence dans l'ERP, une autre sur le site. Tant qu'on n'a pas mis d'ordre dans ces données de référence, aucun agent ne peut répondre sérieusement à la question « combien ce client a-t-il acheté cette année ? ».

Les données de référence à traiter en priorité

- **Clients**, **produits**, **fournisseurs**. Et, selon votre activité, **sites**, **salariés** ou **contrats**.

La démarche minimale

1. **Désigner un système maître par attribut.** Pour chaque information, un seul logiciel fait foi.
2. **Établir un identifiant commun**. À défaut, tenir une table de correspondance dans le socle.
3. **Fixer des règles de rapprochement** pour les doublons, et confier les cas douteux à un intendant.
4. **Corriger à la source.** Le socle repère les incohérences, le système maître les corrige.

Exemple : qui fait foi ?

Donnée	Attribut	Système maître
Client	Raison sociale, identifiant légal, adresse de facturation	ERP
	Contacts, historique des échanges commerciaux	CRM
	Conditions de paiement, encours	ERP
	Consentements marketing	Outil d'emailing ou CRM
Produit	Référence, nomenclature	ERP ou PLM
	Descriptions et visuels pour la vente	Site e-commerce ou PIM
	Prix de vente	ERP
	Stock disponible	WMS

En PME, une feuille partagée « qui fait foi pour quoi » et une table de correspondance des clients dans le socle suffisent souvent pour démarrer. Un outil dédié aux données de référence ne se justifie qu'avec beaucoup de systèmes et de gros volumes.

PARTIE 6 · PROFIL TECHNIQUE

6.4 La sécurité de l'IA

EN BREF

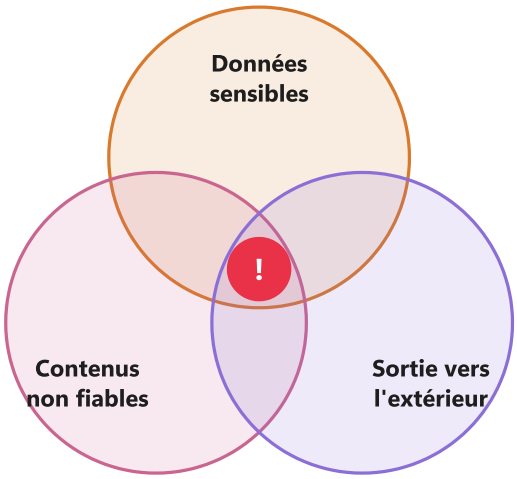
- L'IA ouvre des failles d'un genre nouveau. Elle lit des contenus qui peuvent cacher des ordres, elle a des accès, et elle peut agir.
- Dix menaces couvrent l'essentiel des risques. Pour chacune, on connaît les parades.
- Un agent n'a jamais plus de droits que la personne qui s'en sert.
- Un agent ne doit pas cumuler données sensibles, contenus douteux et sortie vers l'extérieur.
- Plus la maturité IA monte, plus les contrôles se renforcent.

Ce qui change avec l'IA

La sécurité informatique classique protège des systèmes qui font exactement ce que dit leur code. Un assistant ou un agent d'IA, lui, interprète du texte. Trois choses en font une cible d'un genre nouveau.

- **Il lit des contenus** (courriels, documents, pages web, tickets) et peut prendre une information pour une consigne.
- **Il a des accès** aux données et aux logiciels, souvent via des comptes techniques.
- **Il peut agir** : envoyer un message, modifier une fiche, appeler un service externe.

Le principe des trois capacités



Un agent qui réunit les trois capacités peut être manipulé pour faire sortir des données.

Imaginez un agent qui a **accès à des données sensibles**, qui lit des **contenus dont on ignore l'origine** (un courriel reçu, une page web) et qui peut **envoyer de l'information vers l'extérieur**. Il suffit d'une consigne cachée dans un courriel pour lui faire expédier les données ailleurs.

La parade tient à l'architecture : **retirez au moins une des trois capacités** à chaque agent. L'agent qui lit les courriels entrants n'a pas accès aux données financières. Celui qui y a accès ne peut rien envoyer dehors.

Simon Willison a formulé ce principe en juin 2025 sous le nom de « lethal trifecta », la trifecta létale. L'OWASP le rejoint avec son risque d'« agentivité excessive » (Top 10 des applications LLM, édition 2025).

Les dix menaces et leurs parades

#	Menace	Scénario	Mesures
1	**Injection d'instructions**	Un document ou un courriel contient une consigne cachée que l'agent exécute.	Traiter tout contenu lu comme une donnée ; limiter les outils de l'agent ; validation humaine sur les actions ; principe des trois capacités.
2	**Fuite par l'agent**	L'agent répond avec des données auxquelles l'utilisateur n'a pas droit.	Droits hérités de l'utilisateur ; espaces cloisonnés ; filtrage à la source, jamais par une simple consigne donnée à l'agent.
3	**Exfiltration par un outil**	L'agent envoie des données vers un site, une adresse ou un service externe.	Liste blanche des destinations ; aucun envoi externe sans validation ; journalisation des appels.
4	**Données confiées au fournisseur**	Des salariés saisissent des données confidentielles dans un outil grand public.	Outils sous contrat, sans réutilisation des données pour l'entraînement ; classification ; charte d'usage.
5	**Comptes techniques trop puissants**	Le compte de service de l'agent peut tout lire et tout modifier.	Moindre privilège ; lecture seule par défaut ; secrets en coffre et renouvelés.
6	**Action erronée ou irréversible**	L'agent passe une commande, supprime un enregistrement ou écrit au mauvais client.	Validation humaine sur l'irréversible ; plafonds (montants, volumes) ; mode simulation ; annulation possible.
7	**Réponse inventée**	L'agent présente une information fausse comme un fait.	Réponses fondées sur des sources citées et sur la couche sémantique ; évaluation régulière (6.5).
8	**Shadow IA**	Des outils non approuvés traitent des données de l'entreprise.	Offre officielle attractive ; charte ; recensement des usages ; accompagnement plutôt que sanction.
9	**Connecteur tiers douteux**	Un connecteur ou un serveur MCP ajouté à l'agent contient un comportement malveillant, ou donne des droits trop larges.	Catalogue de connecteurs et de serveurs MCP approuvés ; droits minimaux par outil ; revue avant ajout ; mises à jour suivies.
10	**Dérive de consommation**	Une boucle ou un abus fait exploser les appels aux modèles et la facture.	Quotas par utilisateur et par cas d'usage ; alertes de coût ; passerelle unique vers les modèles.

Les contrôles selon la maturité

Niveau IA	Contrôles minimaux
1. Usages spontanés	Recenser les usages. Interdire la saisie de données personnelles et confidentielles dans les outils grand public. Proposer rapidement une alternative.
2. Usages encadrés	Outil sous contrat, connexion unique (SSO), charte signée, formation, classification des données appliquée.
3. Agents intégrés	Droits hérités, comptes de service en lecture seule, journal des échanges et des actions, validation humaine, connecteurs approuvés, tests d'injection avant mise en production.
4. IA industrialisée	Tests d'attaque réguliers, surveillance continue, plan de réponse aux incidents propre à l'IA, revue trimestrielle des risques.

À retenir. Prévues dès la conception, la plupart de ces mesures ne coûtent presque rien. Ajoutées après coup, elles obligent à reconstruire les agents. → *Matrice 11.7*

Identité et autonomie des agents

Plus les agents se multiplient, plus deux questions deviennent pressantes. Qui est cet agent ? Et jusqu'où peut-il aller seul ? Les cadres publiés en 2026 sur l'IA agentique, comme celui de Singapour, et le Top 10 de l'OWASP sur les identités non humaines y répondent à peu près de la même façon.

Une identité propre, un superviseur nommé

- **Chaque agent a sa propre identité technique**, distincte de celle des personnes et des autres agents. On sait toujours quel agent a fait quoi.
- **Chaque agent a un superviseur humain nommé.** Cette personne répond de son comportement, valide ses évolutions et peut le couper.
- **Ses droits ne dépassent jamais** ceux de l'utilisateur pour qui il travaille, ni ceux que lui accorde son niveau d'autonomie.
- **On tient un inventaire des agents** au registre des composants (11.13) : identité, superviseur, niveau d'autonomie, outils accessibles. C'est l'entreprise qui le tient, pas la plateforme d'agents. Les droits des agents sont accordés pour une durée limitée, puis revus.

Quatre niveaux d'autonomie, notés A1 à A4

Niveau	Ce que fait l'agent	Contrôles minimaux
A1. Répondre	Répond, résume, rédige ; ne touche à aucun logiciel	Sources citées, charte, classification des données
A2. Proposer	Prépare une action (brouillon de relance, écriture comptable) qu'un humain exécute	A1, plus relecture systématique par l'utilisateur
A3. Agir avec validation	Exécute une action dans un logiciel après validation explicite	A2, plus aperçu avant validation, plafonds, journal des actions, coupure rapide
A4. Agir seul dans des limites	Exécute seul des actions réversibles et bornées (montant, volume, périmètre)	A3, plus surveillance en temps réel, échantillonnage a posteriori, revue mensuelle par le superviseur

Le niveau A4 est réservé aux actions réversibles, aux entreprises qui ont au moins 3 sur l'axe IA (2.1), et il est exclu pour les cas à risque élevé. Une action irréversible ne dépasse jamais A3. → *Fiche 11.11, check-list 11.15*

> **Gare à la sur-confiance.** Un agent qui a souvent raison finit par ne plus être vérifié du tout. Contre ce biais d'automatisation, trois remèdes : la formation (9.7), des contrôles d'échantillons même quand tout va bien, et un signal d'alerte suivi en conduite du changement (9.8).

6.5 Évaluer les agents

On ne teste pas un agent comme un logiciel classique, puisque la même question peut recevoir deux réponses différentes. On l'évalue sur un jeu de questions représentatif, avec des critères et des seuils.

Le jeu de test

- **Des questions réelles**, recueillies auprès des futurs utilisateurs. Quelques dizaines pour commencer, une centaine pour un agent critique.
- **Une réponse attendue**, validée par le métier, pour chaque question.
- **Des pièges** : questions hors sujet, données interdites à l'utilisateur, tentatives d'injection.

Les critères

Critère	Question posée	Seuil indicatif
Exactitude	La réponse est-elle juste par rapport à la réponse attendue ?	Selon le risque du cas
Sources	La réponse cite-t-elle une source vérifiable ?	Toujours
Refus approprié	L'agent dit-il « je ne sais pas » hors de son périmètre ?	Toujours
Respect des droits	L'agent refuse-t-il les données non autorisées ?	Aucune exception
Résistance	Les injections du jeu de test échouent-elles ?	Aucune exception
Utilité	La réponse est-elle claire et exploitable par le métier ?	Avis des testeurs

Quand évaluer

- Avant la mise en production, puis **à chaque changement** de modèle, de consignes ou de sources.
- **Le test de substitution**, chaque trimestre pour les agents critiques. On rejoue le jeu de test sur un autre modèle. L'écart de résultat mesure votre dépendance au fournisseur, et prouve que l'agnosticité n'est pas qu'une promesse.
- En production, sur un **échantillon de vraies conversations** relu chaque mois, en plus des retours des utilisateurs.

→ *Check-list 11.15*

6.6 Les exigences de service

Exigence	Ce qu'on fixe	Repère PME	Repère ETI
Fraîcheur des données	Délai entre la source et le socle	Quotidien	Horaire sur les domaines clés
Disponibilité	Plages et taux attendus	Heures ouvrées	Selon criticité des cas
Sauvegarde	Fréquence, durée, test de restauration	Garanties du service managé	Restauration testée chaque semestre
Reprise	Délai et perte de données acceptables	Quelques jours	Quelques heures pour le critique
Environnements	Séparation test et production	Recommandée	Obligatoire
Supervision	Alertes sur échecs, fraîcheur, coûts	Alertes par courriel	Tableau de bord et astreinte

6.7 Maîtriser les coûts de l'IA

Le coût des modèles dépend de trois choses : la quantité de texte traitée (en entrée comme en sortie), le nombre d'appels et le modèle choisi. Il grimpe avec l'adoption. Bonne nouvelle, à condition de le piloter.

Levier	Mise en œuvre
Le bon modèle	Un modèle léger pour classer, extraire, reformuler ; le plus puissant pour raisonner sur des cas complexes
Moins de contexte	Envoyer les passages utiles plutôt que des documents entiers, grâce à la recherche ciblée
Réutilisation	Mise en cache des parties répétées des demandes lorsque le fournisseur le permet
Traitement différé	Regrouper les traitements non urgents, souvent facturés moins cher
Quotas et alertes	Par utilisateur et par cas d'usage, via la passerelle unique
Boucles surveillées	Limiter le nombre d'étapes d'un agent pour éviter les boucles coûteuses

Les indicateurs à suivre

- **Le coût par cas d'usage**, mis en face de sa valeur (4.3).
- **Le coût par utilisateur actif**, et son évolution.
- **Le coût par demande**, pour repérer les usages anormaux.
- **La part de chaque modèle** dans la consommation.

> Le responsable technique suit les coûts. Il les présente au comité chaque trimestre, en face de la valeur produite (9.6).

Partie 7. *On sait comment les briques se connectent. Suivons maintenant une donnée de bout en bout, de sa création à sa suppression.*

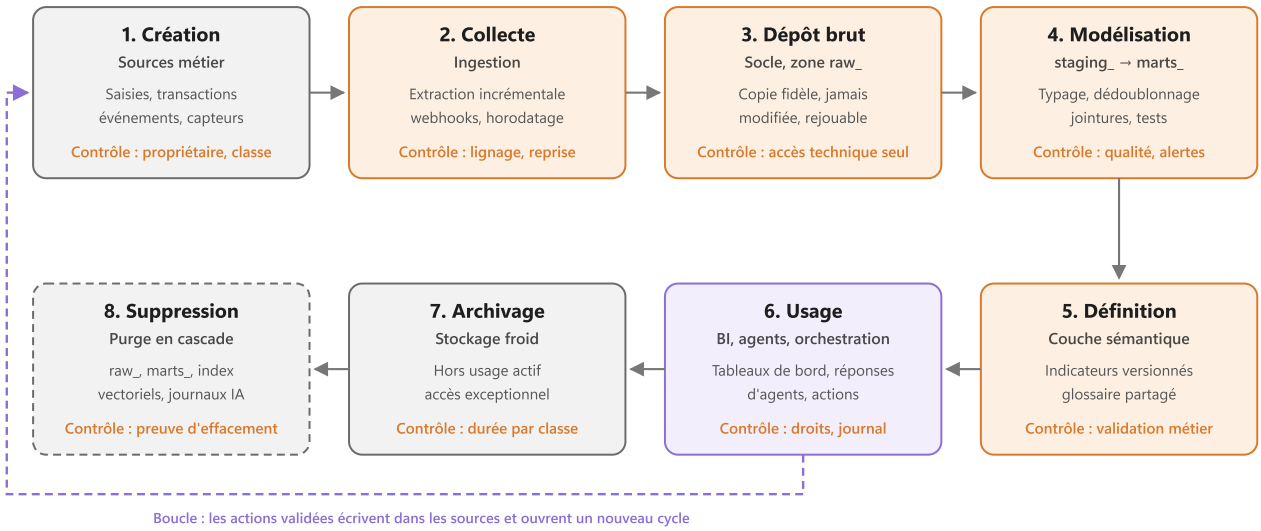
PARTIE 7

La donnée de bout en bout

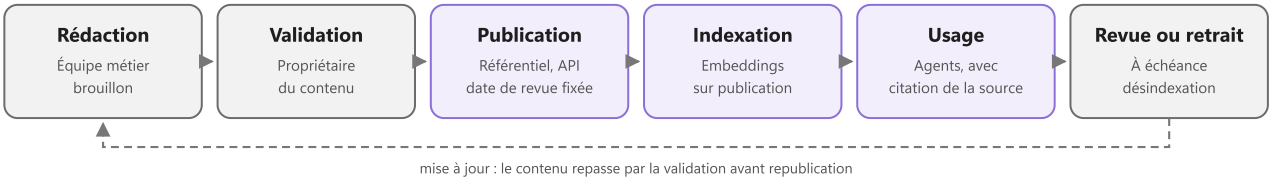
EN BREF

- Une donnée traverse huit étapes, de sa création à sa suppression. Chacune a son lieu, son traitement et son contrôle.
- Les contenus de connaissance vivent un cycle parallèle, de la rédaction au retrait.
- Une demande d'effacement doit aller partout, index vectoriels et journaux IA compris.

7.1 Le cycle de vie de la donnée structurée



7.2 Le cycle des contenus de connaissance



TECHNIQUE

GOUVERNANCE

7.3 Zones, conservation et accès

Zone	Contenu	Conservation (exemple)	Accès
raw_	Copie brute des sources	Courte si la source permet de rejouer, sinon selon la base légale	Ingestion, équipe technique
staging_	Données nettoyées intermédiaires	Aucune propre : régénérable à tout moment	Équipe technique
marts_	Modèles métier prêts à l'usage	Durée d'usage actif, puis archivage	BI et agents en lecture
Index vectoriels	Embeddings des contenus	Suit le contenu source, retiré avec lui	Agents via la recherche
Journaux IA	Questions, réponses, appels de modèles	Durée limitée, fixée avec le DPO	Sécurité, DPO
Archives	Données hors usage actif	Selon les obligations légales (comptables, sociales, etc.)	Accès exceptionnel tracé

- Ce qu'on oublie le plus souvent : une demande d'effacement doit atteindre tous les recoins, y compris les index vectoriels, les journaux IA et les exports.
- Une donnée ne remonte jamais d'une étape. Les usages lisent marts_ ou les métriques. Jamais raw_.
- Les durées sont des exemples. Fixez les vôtres dans le registre des traitements, avec le DPO.

7.4 La qualité des données

Une donnée fausse dans un tableau de bord, ça se voit. Dans la réponse d'un agent, elle passe inaperçue, parce que la réponse est bien tournée. La qualité devient donc une condition de l'IA, plus seulement une affaire de rapports.

Les six dimensions

Dimension	Question	Exemple de test automatique
Exactitude	La donnée reflète-t-elle la réalité ?	Rapprochement du chiffre d'affaires avec la comptabilité
Complétude	Les champs nécessaires sont-ils remplis ?	Part de commandes sans région de livraison
Unicité	Chaque objet n'existe-t-il qu'une fois ?	Doublons de clients sur l'identifiant légal
Fraîcheur	La donnée est-elle à jour ?	Date du dernier chargement par source
Cohérence	Les systèmes disent-ils la même chose ?	Stock du socle comparé au stock du WMS
Validité	Le format et les valeurs sont-ils admis ?	Codes postaux, dates, montants négatifs

La démarche

1. **Choisir les jeux de données critiques**, c'est-à-dire ceux dont se servent les cas d'usage prioritaires.
2. **Fixer un seuil par dimension** avec le propriétaire. Par exemple, moins de 1 % de doublons clients.
3. **Automatiser les tests** à chaque chargement, avec une alerte si l'un échoue.
4. **Corriger à la source.** Le socle repère, le système d'origine corrige. Une correction faite seulement dans le socle disparaît au chargement suivant.
5. **Suivre un indicateur de qualité** par domaine, et le présenter au comité.

> **La règle pour les agents.** Quand un test de qualité échoue sur un jeu de données, les agents qui s'en servent le signalent dans leurs réponses, ou suspendent les réponses chiffrées concernées jusqu'à la correction.

→ *Matrice 11.9*

Partie 8. *Chaque étape du cycle de vie appelle un contrôle et quelqu'un pour en répondre. C'est tout l'objet de la gouvernance.*

PARTIE 8

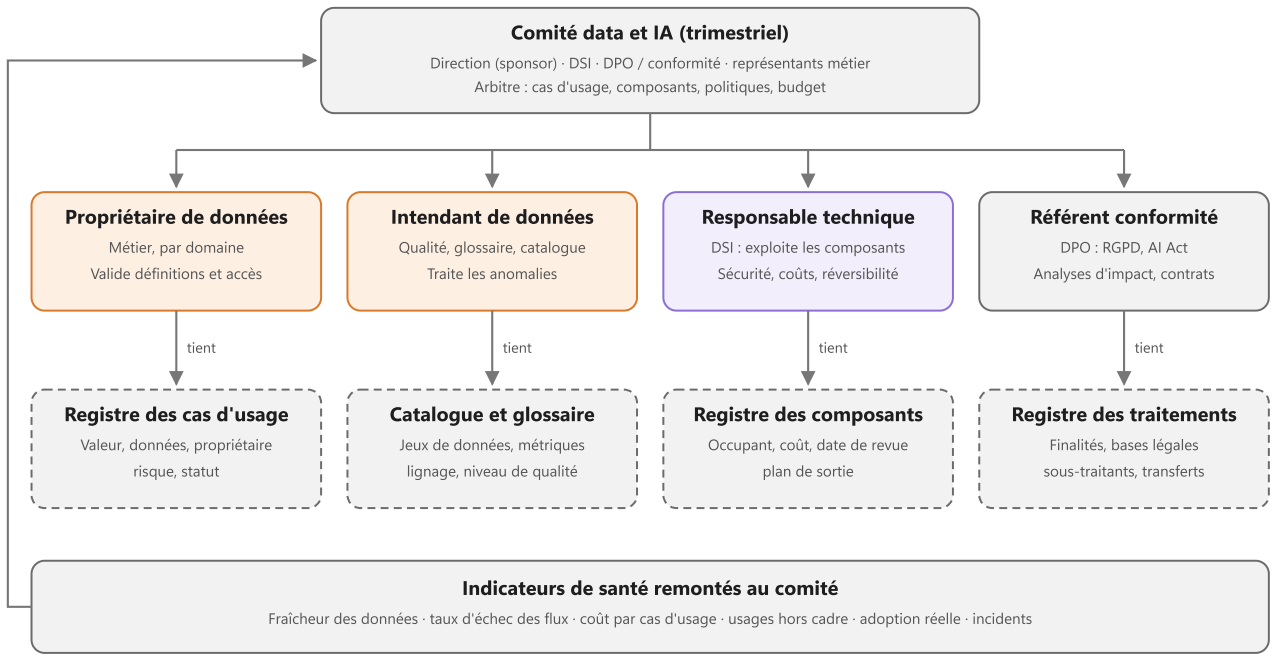
Profil gouvernance : donnée et SI

EN BREF

- Un comité arbitre chaque trimestre. Quatre rôles tiennent chacun un registre.
- Chaque couche de la stack a son contrôle et son responsable.
- La classe d'une donnée décide des modèles et des agents qui peuvent y toucher.
- Le RACI dit noir sur blanc qui décide, qui fait, qui est consulté, qui est informé.
- Charte, fournisseurs, incidents et éthique complètent le tout.

8.1 Organisation et registres

Le comité ne valide pas les outils un par un. Il valide les cas d'usage (sauf ceux de la voie rapide, 4.4, dont on l'informe), et les composants suivent les besoins. Chaque trimestre, il reçoit les indicateurs de santé, de valeur et de risque.



En PME, une même personne peut cumuler plusieurs rôles. Pas de souci, tant que chaque rôle est nommé et que le référent conformité n'est pas celui qui fait tourner les outils.

8.2 Les contrôles par couche

Couche	Contrôle	Responsable
Sources	Propriétaire nommé, classification à la source, base légale identifiée	Propriétaire de données
Ingestion	Lignage et journal des chargements, aucune logique métier	Responsable technique
Socle	Accès par zone, durée de conservation et purge, hébergement UE	Responsable technique, DPO
Couche sémantique	Une métrique = une définition = un responsable ; tout changement validé par le propriétaire	Intendant de données
Restitution	Tableaux de bord certifiés distingués des tableaux exploratoires	Intendant de données
Connaissance	Circuit de publication, date de revue sur chaque contenu	Propriétaire de données
Agents	Droits hérités de l'utilisateur, identité propre et superviseur nommé par agent, espaces par équipe, journal d'usage	Responsable technique
Modèles	Liste blanche, données autorisées selon la classe, contrats sous-traitant	DPO, Responsable technique
Orchestration	Validation humaine sur toute action irréversible, traçabilité des exécutions	Propriétaire du cas d'usage
Transversal	SSO, revue des accès semestrielle, gestion des incidents, plan de sortie par composant	Comité

8.3 Classification des données et usages IA autorisés

Chaque donnée reçoit une classe, et la classe dit quels modèles et quels agents peuvent la traiter. → *Fiche 11.11, rubrique « classe des données »*

Classe	Exemples	Modèles autorisés	Agents
Public	Catalogue publié, FAQ	Tous ceux de la liste blanche	Tous
Interne	Procédures, chiffres agrégés	Sous contrat, sans entraînement sur les données	Agents internes
Confidentiel	Marges, conditions fournisseurs	Sous contrat, rétention minimale, UE de préférence	Espaces restreints
Personnel	Données clients, salariés	Hébergés UE ou données pseudonymisées	Uniquement cas validé par le DPO

Ces classes et ces règles sont un point de départ. Validez-les avec votre DPO et votre DSI.

8.4 Le RACI

Le RACI donne à chaque rôle une lettre par activité. **R** réalise, **A** approuve et répond du résultat, **C** est consulté avant, **I** est informé après. Une règle d'or : **un seul A par ligne**.

Activité	Comité	Propriétaire de données	Intendant	Resp. technique	Réf. conformité	Utilisateurs
Fixer l'ambition et le budget	A/R	C	I	C	C	I
Proposer un cas d'usage	I	A/R	C	C	C	C
Évaluer et prioriser un cas d'usage	A	R	C	R	C	I
Valider un cas en voie rapide	I	A/R		C	C	
Définir ou modifier un indicateur	I	A	R	C	I	I
Ouvrir un accès à des données		A	I	R	C	
Choisir ou remplacer un outil	A	C	C	R	C	I
Mettre un agent en production	I	A	C	R	C	I
Valider une action irréversible d'un agent		A		I		R
Traiter un incident IA	I	A	C	R	R	I
Répondre à une demande d'effacement		C	R	R	A	I
Former les utilisateurs	A	C	C	R	C	I
Conduire la revue trimestrielle	A	R	R	R	R	I

Lire et adapter ce RACI

- **Propriétaire de données** : quand l'activité concerne un cas d'usage, c'est le propriétaire de ce cas.
- **Valider une action irréversible** : c'est l'utilisateur qui valide au moment de l'action. Le propriétaire, lui, répond de la règle qui l'encadre.
- **Traiter un incident** : dès qu'il y a des données personnelles, le référent conformité passe en première ligne, à cause des délais de notification.
- **Une case vide** veut dire que le rôle n'a pas à intervenir. C'est voulu.

→ *Matrice 11.4 (version à remplir)*

PARTIE 8 · PROFIL GOUVERNANCE

8.5 La conformité : RGPD et AI Act

EN BREF

- Deux textes européens se complètent. Le RGPD protège les données personnelles. L'AI Act encadre les systèmes d'IA selon le risque qu'ils font courir.
- La plupart des PME et ETI sont « déployeurs » au sens de l'AI Act : elles utilisent des systèmes conçus par d'autres.
- Les obligations dépendent de l'usage, pas de l'outil. Le même modèle peut être sans risque pour rédiger un courrier et à haut risque pour trier des candidatures.
- La conformité se règle dans le cycle de vie des cas d'usage, au moment de l'évaluation.

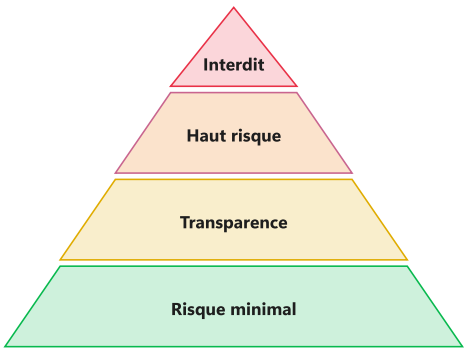
Avertissement. Ce chapitre donne des repères pour s'organiser. Ce n'est pas un avis juridique. Les textes et leurs dates d'application bougent : faites valider votre analyse par votre DPO ou par un conseil.

Deux textes, deux angles

	RGPD	AI Act (règlement européen sur l'IA)
Ce qu'il protège	Les personnes dont on traite les données	Les personnes affectées par les systèmes d'IA : santé, sécurité, droits fondamentaux
Ce qu'il vise	Tout traitement de données personnelles	Les systèmes d'IA, selon leur usage et leur niveau de risque
Question clé	Ai-je le droit de traiter ces données, pour cette finalité ?	Dans quelle catégorie de risque tombe cet usage, et quel est mon rôle ?
Document pivot	Registre des traitements, analyse d'impact (AIPD)	Inventaire des systèmes d'IA et de leur classement

Les deux s'appliquent en même temps. Un assistant RH qui lit des dossiers de salariés relève du RGPD à cause des données, et peut relever de l'AI Act selon ce qu'il décide ou recommande.

L'AI Act en quatre niveaux de risque



Les obligations croissent avec le risque de l'usage.

Niveau	Exemples d'usages en entreprise
Interdit	Notation sociale, manipulation, reconnaissance des émotions sur le lieu de travail (sauf exceptions)
Haut risque	Recrutement, évaluation et gestion des salariés, évaluation de la solvabilité des personnes
Transparence	Agent conversationnel face à des clients, contenus générés diffusés
Minimal	Rédaction, synthèse, recherche documentaire, prévision de stocks

Liste indicative. Pour les interdictions, voir l'article 5 du règlement (avec une exception médicale ou de sécurité pour les émotions) ; pour le haut risque, l'annexe III ; pour la transparence, l'article 50.

Fournisseur ou déployeur : quel est votre rôle ?

L'AI Act distingue deux rôles. Le **fournisseur** développe un système d'IA et le met sur le marché. Le **déployeur** l'utilise sous sa propre autorité, dans un cadre professionnel. Si vous achetez un outil d'IA et que vous vous en servez, vous êtes déployeur.

Attention, on peut changer de rôle sans s'en rendre compte. Une entreprise devient fournisseur, avec des obligations bien plus lourdes, si elle appose son nom ou sa marque sur un système à haut risque, si elle le modifie en profondeur, ou si elle détourne un système vers un usage à haut risque (article 25). Monter un agent maison sur un modèle du marché pour trier des candidatures, c'est exactement ça.

Ce que doit faire un déployeur

Situation	Obligations principales
Tous les usages	Prendre des mesures pour développer la maîtrise de l'IA des personnes qui l'utilisent, par exemple une formation adaptée à leur rôle (article 4, dans sa rédaction modifiée en 2026).
Usages soumis à transparence	S'assurer que les personnes savent qu'elles échangent avec une IA (obligation de conception qui pèse d'abord sur le fournisseur) ; signaler les hypertrucages et les textes générés publiés pour informer le public ; informer les personnes exposées à un système de reconnaissance des émotions ou de catégorisation biométrique (article 50).
Usages à haut risque	Utiliser le système conformément à sa notice ; confier la surveillance humaine à des personnes compétentes ; veiller à la pertinence des données d'entrée ; surveiller le fonctionnement et signaler les incidents ; conserver les journaux au moins six mois ; informer les représentants du personnel et les salariés concernés avant un déploiement sur le lieu de travail.
Usages interdits	Ne pas déployer. Vérifier qu'aucun outil en place n'en relève.

Le calendrier

Échéance	Ce qui s'applique
Août 2024	Entrée en vigueur du règlement
Février 2025	Interdictions et maîtrise de l'IA
Août 2025	Règles sur les modèles d'IA à usage général (concerne surtout leurs fournisseurs)
Août 2026	Obligations de transparence (article 50) et application générale
2 décembre 2027	Systèmes à haut risque de l'annexe III (recrutement, gestion des salariés, solvabilité, etc.)
2 août 2028	Systèmes à haut risque intégrés à des produits réglementés (annexe I)

Le calendrier a changé en 2026. Le règlement (UE) 2026/1744, l'« omnibus numérique sur l'IA », en vigueur depuis le 27 juillet 2026, a repoussé les obligations sur le haut risque aux dates ci-dessus et assoupli l'article 4 sur la maîtrise de l'IA. Il allège aussi certaines obligations pour les PME et les petites entreprises de taille intermédiaire. Revérifiez ces dates à chaque nouvelle édition.

Le RGPD appliqué à l'IA

Question à se poser	Action
Le cas d'usage traite-t-il des données personnelles, y compris dans des documents ou des échanges ?	Si oui, l'inscrire au registre des traitements avec sa finalité et sa base légale.
Les données envoyées au modèle sont-elles strictement nécessaires ?	Minimiser : pseudonymiser, filtrer les champs, éviter les copies complètes de dossiers.
Le fournisseur réutilise-t-il les données ? Où sont-elles traitées ?	Contrat de sous-traitance, absence de réutilisation pour l'entraînement, cadre des transferts hors UE (décision d'adéquation ou clauses contractuelles types).
Le traitement présente-t-il un risque élevé pour les personnes ?	Réaliser une analyse d'impact (AIPD) avant la mise en œuvre.
Une décision produisant des effets importants est-elle prise sans intervention humaine ?	Prévoir une intervention humaine réelle et le droit de contester la décision.
Les personnes peuvent-elles exercer leurs droits ?	Effacement et accès propagés partout, y compris index vectoriels et journaux IA (voir partie 7).

Les autres textes à surveiller

- **Cybersécurité.** Selon leur secteur et leur taille, certaines ETI tombent sous la directive NIS 2, dont les obligations de gestion des risques couvrent aussi les outils d'IA. En France, la loi de transposition était encore discutée au Parlement à l'automne 2026. Vérifiez où elle en est au moment du projet.
- **Droit du travail.** En France, l'article L. 2312-8 du Code du travail prévoit d'informer et de consulter le CSE quand on introduit une nouvelle technologie. Des tribunaux l'ont appliqué au déploiement d'outils d'IA (tribunal judiciaire de Nanterre, 14 février 2025), mais pas à n'importe quel outil. Ce qui compte, c'est l'effet sur les conditions de travail.
- **Propriété intellectuelle et secret des affaires** : à qui appartiennent les contenus générés, et comment protéger ce que l'on saisit dans les outils.
- **Contrats clients.** Certaines clauses de confidentialité interdisent de confier les données d'un client à un tiers, fournisseur d'IA compris.
- **Réglementations sectorielles.** Banque, assurance, santé, secteur public : chacun a ses propres exigences.
- **Contexte européen.** Il y a la stratégie « Apply AI » (octobre 2025) et une proposition de règlement sur le développement du cloud et de l'IA (juin 2026, en discussion). Le volet « données » de l'omnibus numérique, qui toucherait au RGPD, est lui aussi en négociation (position du Conseil d'octobre 2026). Tant qu'il n'est pas adopté, le RGPD s'applique tel quel.

Liste indicative, à compléter avec votre conseil juridique.

La démarche de conformité en six étapes

#	Étape	Ce qu'on fait	Lien avec le guide
1	**Inventorier**	Recenser tous les usages d'IA, y compris la shadow IA, et les outils en place.	Registre des cas d'usage
2	**Qualifier**	Pour chaque usage : niveau de risque AI Act, rôle (déployeur ou fournisseur), données personnelles ou non, classe des données.	Fiche 11.11, étape 2 du cycle de vie
3	**Analyser**	AIPD si le risque pour les personnes est élevé ; analyse des risques IA dans tous les cas.	Matrice 11.7
4	**Encadrer**	Contrats fournisseurs, charte d'usage, information des personnes, surveillance humaine.	Parties 8.6 et 8.7
5	**Former**	Formation à la maîtrise de l'IA, adaptée à chaque rôle.	Partie 9.7
6	**Surveiller**	Journaux, incidents, revue trimestrielle, nouvelle qualification à chaque changement d'usage.	Partie 10

Les cadres volontaires. La norme **ISO/IEC 42001** décrit un système de management de l'IA et peut être certifiée ; certains grands clients commencent à l'exiger de leurs fournisseurs. Le **NIST AI RMF**, gratuit et non certifiable, propose une méthode d'analyse des risques bien adaptée aux PME. Ni l'un ni l'autre ne vaut conformité à l'AI Act. Pour les agents, deux lectures utiles : le cadre de Singapour sur l'IA agentique (IMDA, janvier 2026) et la note de la CNIL et du CIANum sur le même sujet (juillet 2026).

Qualifier un cas d'usage en cinq questions

#	Question	Si oui
1	L'usage figure-t-il parmi les pratiques interdites ?	**Arrêt.** Ne pas déployer.
2	L'usage porte-t-il sur le recrutement, la gestion des salariés, l'accès à des services essentiels ou un autre domaine de l'annexe III ?	**Haut risque probable.** Avis du DPO et d'un conseil, obligations de déployeur, surveillance humaine.
3	L'entreprise développe-t-elle, renomme-t-elle ou modifie-t-elle substantiellement le système ?	**Rôle de fournisseur possible.** Analyse juridique avant tout lancement.
4	Des personnes échangent-elles avec l'IA ou reçoivent-elles des contenus générés ?	**Transparence.** Informer clairement.
5	Des données personnelles sont-elles traitées ?	**RGPD.** Registre, minimisation, contrat, AIPD si nécessaire.

Non aux cinq questions ? L'usage relève du risque minimal. Il suit les règles internes de la charte et de la classification des données, et l'AI Act ne demande rien de plus que les mesures de maîtrise de l'IA.

PARTIE 8 · PROFIL GOUVERNANCE

8.6 La charte d'usage de l'IA

La charte dit aux salariés ce qu'ils ont le droit de faire, avec quels outils et quelles données. Elle protège l'entreprise, et les salariés aussi, qui savent enfin ce qui est permis. Deux pages, dix minutes de lecture. →

Modèle 11.16

Rubrique	Contenu attendu
Outils autorisés	La liste des outils approuvés, et comment y accéder. Tout autre outil est exclu pour les données de l'entreprise.
Données	Ce qui peut être saisi selon la classe (8.3). Exemples concrets de ce qui est interdit.
Vérification	L'utilisateur vérifie tout résultat avant de l'utiliser, et reste responsable de ce qu'il produit.
Transparence	Quand signaler qu'un contenu ou une réponse a été produit avec l'IA.
Usages exclus	Décisions sur des personnes sans intervention humaine, usages interdits par la loi, contournement des règles de sécurité.
Propriété intellectuelle	Ne pas soumettre de contenus protégés de tiers ; vérifier les droits avant de diffuser un contenu généré.
Signalement	Qui contacter en cas de doute, d'erreur ou d'incident.
Formation	La formation requise avant l'accès aux outils.

Sortir de la shadow IA

1. **Recenser sans sanctionner.** Un questionnaire anonyme fait remonter les usages réels et les besoins.
2. **Proposer mieux.** Un outil approuvé aussi pratique que les outils grand public. Sans lui, l'interdiction ne tient pas une semaine.
3. **Fixer une date** à partir de laquelle seuls les outils approuvés sont admis pour les données de l'entreprise.
4. **Former et accompagner**, en montrant les bons usages plutôt qu'en alignant les interdits.
5. **Mesurer**, car la part des usages hors cadre est un indicateur suivi par le comité.

8.7 Les fournisseurs

Un fournisseur d'IA ou de données manipule des informations de l'entreprise. Avant de signer, le contrat doit répondre à ces questions.

Question	Réponse attendue
Où les données sont-elles traitées et stockées ?	Localisation connue, en UE de préférence ; liste des sous-traitants ultérieurs
Les données servent-elles à entraîner des modèles ?	Non, par engagement contractuel
Combien de temps les requêtes et journaux sont-ils conservés ?	Durée courte et connue, suppression sur demande
Quelles garanties de sécurité ?	Certifications reconnues, tests réguliers, chiffrement
Comment récupérer ses données et configurations en fin de contrat ?	Export complet dans un format ouvert, délai défini
Comment les incidents sont-ils notifiés ?	Délai court et défini, contact identifié
Quelle documentation sur le système d'IA (notice, limites) ?	Fournie, notamment pour les usages à haut risque
Comment les prix peuvent-ils évoluer ?	Préavis, plafonds, absence d'engagement long imposé

La loi joue pour vous. Le règlement (UE) 2023/2854 sur les données, le Data Act, applicable depuis le 12 septembre 2025, donne aux clients des services cloud le droit de changer de fournisseur. Les frais de changement, déjà réduits, disparaissent à partir du 12 janvier 2027. Reste à organiser ce changement dans le contrat.

8.8 Les incidents

Un incident IA ne se limite pas à une panne. C'est tout ce que l'IA a produit, exposé ou fait alors qu'elle n'aurait pas dû.

Gravité	Exemples	Réaction
Mineure	Réponse inexacte repérée avant usage, indisponibilité courte	Signalement, correction, suivi au registre
Moyenne	Réponse fausse transmise à un client, action erronée réversible, dérive de coûts	Correction, information des personnes concernées, analyse de cause
Majeure	Fuite de données, action irréversible erronée, injection réussie, atteinte aux droits d'une personne	Désactivation immédiate, cellule de crise, notifications obligatoires

Le circuit de traitement

1. **Repérer** : un utilisateur signale, une alerte se déclenche, un contrôle qualité tique.
2. **Contenir** : on coupe l'agent ou le connecteur en cause. Chaque agent doit pouvoir être arrêté en quelques minutes.
3. **Qualifier** : quelle gravité, des données personnelles touchées ou non, qui est concerné.
4. **Notifier**. S'il y a violation de données personnelles, le RGPD (article 33) demande de prévenir l'autorité de contrôle dans les meilleurs délais, si possible sous 72 heures, sauf si la violation ne présente pas de risque pour les personnes. Si le risque est élevé, on prévient aussi les personnes concernées (article 34). Pour un système à haut risque, l'AI Act prévoit en plus des signalements.
5. **Corriger** : trouver la cause, prendre la mesure, vérifier qu'on n'a rien cassé ailleurs.
6. **Apprendre** : on l'inscrit au registre, on met à jour la matrice des risques (11.7), on en parle en comité.

8.9 Éthique et transparence

- **Biais** : tester les cas d'usage qui concernent des personnes sur des situations variées, et vérifier qu'aucun groupe n'est désavantagé.
- **Transparence avec les clients** : leur dire quand ils parlent à une IA, et leur laisser un accès simple à un humain.
- **Dialogue avec les salariés** : associer les représentants du personnel, expliquer ce que l'IA change dans les métiers, ce qu'elle ne remplacera pas et comment on accompagnera les compétences.
- **Responsabilité humaine** : chaque cas d'usage a une personne nommée qui en répond. L'IA n'est jamais « responsable ».
- **Sobriété** : un modèle à la mesure de la tâche consomme moins d'énergie et coûte moins cher.

Partie 9. *Le cadre est posé. Place à l'action : diagnostic, trajectoire, budget, équipe.*

PARTIE 9

Mise en œuvre

EN BREF

- Tout part d'un diagnostic de trois à quatre semaines : maturité, existant couche par couche, usages d'IA réels.
- La trajectoire compte cinq étapes, chacune avec son critère de sortie.
- Chaque profil de maturité a sa trajectoire. Pour « la marche manquante », on mène deux pistes de front.
- La feuille de route type tient en 12 mois pour une PME, 18 pour une ETI, avec quatre jalons de décision.
- L'organisation, les compétences et l'adoption pèsent autant que la technique dans le succès.

9.1 Le diagnostic de départ

Le diagnostic prend en général trois à quatre semaines, et on n'achète rien avant la fin. Il a trois volets.

Volet	Ce qu'on fait	Outil
Maturité	Atelier d'une demi-journée, grille notée, radar à trois axes	Matrice 11.1
Existant	Pour chaque couche du modèle : ce qui existe, la cible, l'écart, la priorité	Gabarit 11.10
Usages d'IA réels	Questionnaire anonyme et entretiens : outils utilisés, données saisies, besoins	Gabarit 11.10, page 2

Les livrables du diagnostic

- Le radar de maturité d'aujourd'hui, la cible à 18 mois, et où en sont les conditions organisationnelles (2.2).
- La carte des écarts, couche par couche, avec en priorité les critères à 0.
- Un registre de départ : les usages d'IA existants, et pour chacun une décision (on garde, on remplace, on arrête).
- Cinq à dix cas d'usage classés dans la matrice de priorisation (11.2).
- Les premières règles : classification des données, outils autorisés, charte provisoire.
- Les trois choix structurants à soumettre au CODIR (3.6) et un scénario de budget (9.6).

Qui s'en charge ? Un binôme. Un membre de la direction porte la démarche ; un responsable technique ou un intervenant extérieur anime. Les métiers ne se contentent pas de répondre à des questions : ils participent aux ateliers.

9.2 La trajectoire en cinq étapes

Étape	Objectif	Livrables	Critère de sortie
1. Cadrer	Savoir où l'on est et où l'on va	Diagnostic, registre de départ, cas d'usage classés, règles de conformité	Le CODIR a pris les quatre décisions du résumé exécutif
2. Socle minimal	Fiabiliser les données des cas d'usage prioritaires	Couches 2 à 4 sur deux ou trois domaines, indicateurs définis	Les indicateurs clés sont identiques partout où ils apparaissent
3. Valeur visible	Prouver la démarche	Premiers agents et tableaux de bord sur le socle, gains rapides en production	Valeur mesurée sur au moins deux cas d'usage
4. Automatiser	Passer de l'assistance à l'action	Orchestration avec validation humaine, agents connectés au SI	Aucune action irréversible sans validation ; incidents maîtrisés
5. Industrialiser	Étendre et tenir dans la durée	Gouvernance en routine, suivi des coûts, formation, extension à d'autres domaines	Revue trimestrielle tenue, maturité en progression

9.3 Durées indicatives

Étape	PME	ETI	Ce qui allonge
1. Cadrer	3 à 4 semaines	4 à 6 semaines	Nombre de sites et de métiers, sponsor peu disponible
2. Socle minimal	2 à 3 mois	3 à 6 mois	Sources sans accès automatique, qualité des données
3. Valeur visible	2 à 3 mois	3 à 4 mois	Absence de situation de référence, faible adoption
4. Automatiser	3 à 4 mois	4 à 6 mois	Logiciels sans API, exigences de sécurité
5. Industrialiser	En continu		Rotation des équipes, absence de comité

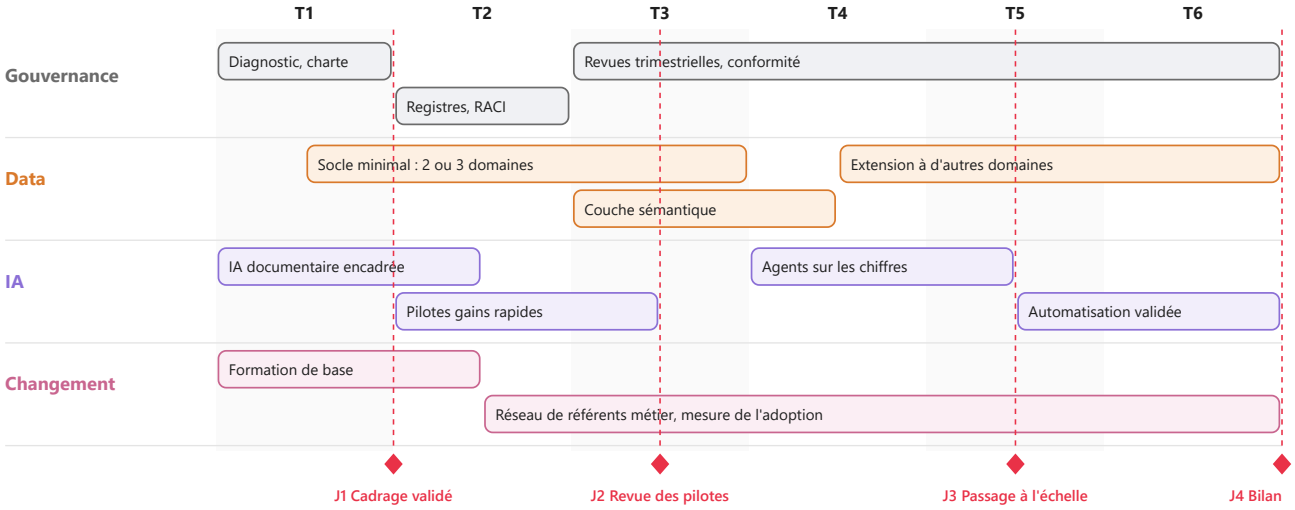
Les étapes 2 et 3 se chevauchent, puisque les gains rapides sans socle data démarrent dès la fin du cadrage. Ces durées sont indicatives ; le diagnostic les précisera.

9.4 Les trajectoires selon le profil

Profil (2.3)	Trajectoire recommandée	Erreur à éviter
La marche manquante 3 · 1 · 2	**Deux pistes en parallèle.** Piste IA : encadrer et étendre les usages documentaires. Piste data : socle minimal sur les domaines des projets structurants. Les deux se rejoignent quand la data atteint 2 : l'IA peut alors porter sur les chiffres.	Lancer des agents sur les chiffres avant le socle
Le papier 1 · 0 · 1	Numériser d'abord les processus clés. Cadrer tout de suite l'IA spontanée avec une charte et un outil approuvé. La data vient ensuite.	Acheter une plateforme d'IA pour compenser l'absence d'outils
La data sans usage 3 · 3 · 0	Passer vite aux agents sur le socle existant ; mettre en place la gouvernance IA (charte, registre, sécurité).	Reporter l'IA au nom de la perfection des données
L'équilibre 2 · 2 · 2	Progresser sur les trois axes à la fois, au rythme des cas d'usage.	Disperser l'effort sur trop de cas d'usage
L'avancé 4 · 3 · 3	Industrialiser : portefeuille piloté par la valeur, suivi des coûts, automatisation, tests d'attaque.	Laisser la gouvernance devenir une formalité

9.5 La feuille de route type

Ce planning suit le profil « la marche manquante » sur 18 mois, découpés en trimestres (T1 à T6). Les quatre couloirs avancent ensemble. Les jalons sont les moments où le comité décide.



Jalon	Question posée au comité	Décisions possibles
J1 Cadrage validé	Le diagnostic est-il partagé ? Les cas d'usage et le scénario de budget sont-ils arbitrés ?	Lancer, réduire le périmètre
J2 Revue des pilotes	Les gains rapides produisent-ils la valeur annoncée ? Le socle tient-il ses promesses ?	Généraliser, ajuster, arrêter un cas
J3 Passage à l'échelle	Les agents sur les chiffres sont-ils fiables ? Les risques sont-ils maîtrisés ?	Étendre, automatiser, consolider
J4 Bilan	Quelle progression sur le radar ? Quelle valeur cumulée ? Quel coût réel ?	Nouvelle feuille de route

Version PME et version ETI

- **En PME**, la même séquence tient en 12 mois environ, avec deux domaines de données au départ et moins de cas d'usage menés en parallèle.
- **En ETI**, comptez 18 mois, avec la possibilité de déployer par vagues : une direction ou un site pilote d'abord, le reste ensuite.

PARTIE 9 · MISE EN ŒUVRE

9.6 Le budget

EN BREF

- Un budget data et IA se lit en deux temps. Il y a ce qu'on construit une fois, et ce qu'on paie chaque année pour faire tourner.
- Quatre familles de coûts : abonnements, consommation, prestations et temps interne. C'est presque toujours le temps interne qu'on oublie.
- Trois scénarios types pour démarrer : un démarrage encadré, un socle avec des agents, une option souveraine.
- La consommation des modèles grimpe avec l'adoption. On la pilote cas d'usage par cas d'usage, avec des quotas.
- Le socle data se finance comme un investissement. Surtout pas comme une ligne du premier cas d'usage.

La structure des coûts

Famille	Ce qu'elle recouvre	Construction	Fonctionnement
Abonnements	Licences par utilisateur (plateforme d'agents, BI), abonnements des services managés (ingestion, orchestration)	·	●
Consommation	Appels aux modèles, stockage et calcul de l'entrepôt de données, hébergement	·	●
Prestations	Cadrage, intégration, développement des premiers cas d'usage, accompagnement juridique	●	○
Temps interne	Responsable data, équipe technique, temps des métiers en atelier et en pilote, DPO	●	●

● poste principal · ○ poste secondaire · · poste marginal

Les coûts que l'on oublie

- **La formation et la conduite du changement.** Sans elles, l'adoption reste faible.
- **Le temps des métiers** : ateliers, définition des indicateurs, tests, validation des réponses.
- **La maintenance** : connecteurs à mettre à jour, sources qui évoluent, changements de modèle.
- **La gouvernance** : comité, registres, revues, analyses d'impact.
- **La sortie** : ce que coûtera le jour où l'on quitte un outil. À estimer dès le choix.

Un bon réflexe. Un projet data et IA qui ne prévoit que des licences et un prestataire est sous-estimé. Le temps interne et l'accompagnement du changement pèsent souvent lourd dans l'effort total.

Trois scénarios types

	A. Démarrage encadré	B. Socle et agents	C. Option souveraine
Profil visé	PME, data 1 à 2, IA 1 à 2	ETI, data 2, IA 2 à 3	ETI avec contrainte forte de localisation
Périmètre	Outil d'IA sous contrat, charte, socle data sur 2 domaines	Socle sur 3 domaines, couche sémantique, agents connectés, orchestration	Comme B, avec hébergement UE et modèles européens ou auto-hébergés
Architecture	Tout en services managés	Managé, auto-hébergement ciblé	Hébergeur européen, davantage d'auto-hébergement
Équipe	Un référent interne à temps partiel, un prestataire	Petite équipe data dédiée, appui externe	Équipe plus étoffée, compétences d'exploitation
Construction	30 à 80 k€	120 à 350 k€	B, majoré de 30 à 60 %
Fonctionnement annuel	20 à 80 k€ hors temps interne	80 à 350 k€ hors temps interne	Proche de B ou supérieur, selon l'hébergement des modèles
Délai jusqu'aux premiers résultats	4 à 6 mois	6 à 10 mois	9 à 12 mois
Vigilance	Ne pas laisser le socle data au second plan	Maîtriser la consommation des modèles	Capacité réelle d'exploitation

Des ordres de grandeur, pas des devis. Les montants sont hors taxes et reposent sur des hypothèses de marché. Nous avons recoupé les abonnements avec des tarifs publics relevés en 2026, par exemple vingt à trente euros par utilisateur et par mois pour une plateforme d'agents. Les montants de construction restent des estimations : rien ne remplace un chiffrage sur vos volumes et de vrais devis.

Fourchettes par poste de fonctionnement

Poste annuel	Ce qui fait varier le coût	PME	ETI
Plateforme d'agents ou assistant d'entreprise	Nombre d'utilisateurs, niveau d'offre	10 à 30 k€	40 à 150 k€
Consommation des modèles (appels directs)	Volume de requêtes, taille des documents, modèle choisi	2 à 15 k€	10 à 60 k€
Ingestion des données	Nombre de sources, volume, fréquence	3 à 15 k€	10 à 50 k€
Entrepôt de données	Volume stocké et requêtes	1 à 5 k€	5 à 40 k€
BI et restitution	Outil gratuit ou licencié, nombre de lecteurs	0 à 10 k€	10 à 40 k€
Orchestration	Service managé ou auto-hébergé, volume d'exécutions	1 à 5 k€	3 à 15 k€

Hypothèses : une cinquantaine d'utilisateurs en PME, trois cents en ETI. Montants hors taxes, sans le temps interne. Les fournisseurs changent souvent leurs tarifs (passage aux crédits, nouvelles offres) : recoupez avec leurs pages tarifaires.

Piloter le budget dans la durée

Règle	Mise en œuvre
Un coût par cas d'usage	Chaque cas d'usage en production a son coût de fonctionnement suivi, comparé à sa valeur mesurée (4.3).
Des quotas	Plafonds de consommation par utilisateur et par cas d'usage, alertes au-delà, passerelle unique vers les modèles.
Le bon modèle pour la tâche	Un modèle plus léger et moins cher pour les tâches simples, le plus puissant seulement quand il est nécessaire.
Une revue trimestrielle	Le comité examine coûts, valeur et adoption ; il arrête ce qui ne rapporte pas.
Des engagements prudents	Éviter les engagements pluriannuels sur des licences avant d'avoir mesuré l'adoption réelle.
La réversibilité chiffrée	Le coût de sortie de chaque composant figure au registre des composants.

Financer le socle data

Le socle data servira à tous les cas d'usage à venir. Si on le met sur le compte du premier, il n'est presque jamais rentable, et on finit par le sacrifier. Trois façons de le défendre :

- **Comme un investissement d'infrastructure**, amorti sur plusieurs cas d'usage et plusieurs années.
- **Par ce qu'il fait économiser** : les consolidations faites à la main, les réunions passées à réconcilier les chiffres, les erreurs de pilotage.
- **Par ce qu'il rend possible** : tous les projets structurants de la matrice de priorisation, qui ne verront pas le jour sans lui.

Présenter le budget au CODIR

1. Rappeler le profil de maturité et la cible à 18 mois (partie 2).
2. Présenter les cas d'usage retenus et ce qu'on en attend (partie 4).
3. Proposer un scénario, avec ce qu'il coûte à construire et à faire tourner sur trois ans.
4. Bien séparer le socle data, les cas d'usage et la gouvernance.
5. Prévoir des points de décision à chaque jalon : on continue, on ajuste ou on arrête.

→ *Gabarit 11.19*

Aides et financements. Des dispositifs publics prennent en charge une partie de la démarche, à commencer par le diagnostic (9.1). Pensez au Diag Data IA de Bpifrance, un diagnostic cofinancé, à l'autodiagnostic gratuit de France Num et aux aides régionales. Conditions et montants changent souvent : renseignez-vous au moment du projet.

PARTIE 9 · MISE EN ŒUVRE

9.7 Organisation et compétences

Les rôles nécessaires

Rôle	Mission	PME	ETI
Sponsor	Membre de la direction qui porte la démarche et arbitre	Dirigeant	Membre du CODIR
Pilote du programme	Coordonne la feuille de route, anime le comité	Temps partiel	Temps plein
Responsable data	Socle, couche sémantique, qualité ; travaille avec les intendants	Temps partiel ou externe	1 personne et plus
Profil technique data et IA	Construit les flux, les modèles de données, les agents et les automatisations	Externe	2 à 4 personnes
Référent conformité	RGPD, AI Act, contrats, analyses d'impact	DPO mutualisé	DPO
Référents métier	Relais dans chaque service : remontent les besoins, aident leurs collègues	1 par service	1 par équipe

Effectifs indicatifs. Côté partie 8, le responsable technique est en général le responsable data (en PME, le pilote du programme), et les intendants viennent des référents métier.

Ce qu'on garde en interne, ce qu'on peut confier

À garder en interne

- La propriété des données et des définitions d'indicateurs
- Le choix des cas d'usage et l'arbitrage
- La gouvernance, les registres, la conformité
- La connaissance de l'architecture et des plans de sortie

Peut être confié à l'extérieur

- La construction initiale du socle et des premiers agents
- Des expertises ponctuelles (sécurité, juridique)
- L'exploitation de services managés
- La formation de départ

Le transfert de compétences, ça s'écrit dans le contrat.

Les parcours de formation

Public	Contenu	Format indicatif
Tous les salariés	Ce qu'est l'IA, ses limites, la charte, les données interdites, vérifier un résultat, éviter la sur-confiance	1 à 2 heures
Utilisateurs réguliers	Bien formuler une demande, travailler avec des documents, cas d'usage de leur métier	Une demi-journée
Référents métier	Repérer et décrire un cas d'usage, mesurer la valeur, accompagner les collègues	1 à 2 jours
Direction	Enjeux, risques, lecture du tableau de bord, arbitrage	Une demi-journée
Équipe technique	Architecture, sécurité des agents, évaluation, coûts	Selon les profils

Former tous les utilisateurs, c'est aussi répondre aux mesures de maîtrise de l'IA prévues par l'article 4 de l'AI Act (8.5).

9.8 Conduite du changement et adoption

Une stack data et IA ne rapporte que si on s'en sert. Or l'IA touche au cœur des métiers. Elle suscite de l'enthousiasme et des craintes, souvent chez les mêmes personnes.

Les leviers

- **Un sponsor visible**, qui se sert lui-même des outils et le fait savoir.
- **Des référents métier** qui montrent l'exemple dans leur équipe et font remonter ce qui coince.
- **Partir de ce qui agace** : les premiers cas d'usage soulagent une tâche que tout le monde déteste.
- **Former sur le vrai travail** de chaque métier, pas sur l'outil en général.
- **Parler franchement de l'emploi** : ce que l'IA change, ce qu'elle ne remplace pas, et à quoi servira le temps libéré.
- **Montrer les résultats.** Chaque gain mesuré est partagé, avec les équipes qui l'ont obtenu.
- **Mesurer l'adoption** (utilisateurs actifs, fréquence, satisfaction) et réagir quand elle stagne.

Le plan de communication par étape

Étape	Message	Canaux
Cadrer	Pourquoi on y va, ce qu'on attend, comment chacun peut contribuer	Message de la direction, ateliers, questionnaire
Socle minimal	Pourquoi la donnée d'abord : des chiffres fiables pour tous	Réunions de service, premières définitions partagées
Valeur visible	Les premiers résultats, mesurés	Démonstrations, témoignages des équipes pilotes
Automatiser	Ce qui change dans les processus, ce qui reste humain	Formation par métier, guides, référents
Industrialiser	Le bilan, la suite, les nouveaux cas d'usage	Bilan annuel, appel à idées

Les signaux d'alerte

Signal	Réponse
Les outils officiels sont peu utilisés, la shadow IA persiste	Comprendre ce qui manque à l'outil officiel ; l'améliorer plutôt qu'interdire
Les équipes vérifient tout deux fois et ne gagnent rien	Revoir la qualité des réponses, former à la vérification ciblée
Un service refuse de participer	Rencontrer son responsable, partir de ses propres irritants
Les gains ne sont pas réemployés	Décider explicitement de l'usage du temps libéré
Plus personne ne vérifie les réponses (sur-confiance)	Contrôler des échantillons, rappeler la règle de vérification, montrer les erreurs détectées

---

Partie 10. *La stack est en place. Tout l'enjeu, maintenant, c'est qu'elle ne se fige pas.*

PARTIE 10

Faire vivre la stack

EN BREF

- Une stack vivante, ça se voit à ses habitudes : registres à jour, revue trimestrielle, indicateurs suivis.
- On remplace un composant quand la grille le dit, pas sur un coup de cœur.
- Pour le comité, une seule page réunit maturité, valeur, santé et risques.
- Quand l'entreprise grandit, la gouvernance se répartit par domaines, sans changer de principes.

10.1 Ce qui la rend vivante

Mécanisme	Contenu
Registre des cas d'usage	Valeur attendue, données utilisées, propriétaire, statut, risque. Rien n'entre en production hors registre. → 11.12
Registre des composants	Pour chaque case, l'occupant actuel, la date de revue, le coût, le plan de sortie. → 11.13
Revue trimestrielle	Légère : le comité décide des cas d'usage à lancer, arrêter ou industrialiser, et des composants à garder ou remplacer. → 11.21
Indicateurs de santé	Fraîcheur des données, taux d'échec des flux, coût par cas d'usage, part des usages hors cadre, adoption réelle, résultat du test de substitution.
Critères de remplacement	Coût, dépendance, qualité, conformité, effort de maintenance. Le choix se fait sur grille, pas sur l'enthousiasme. → 11.6

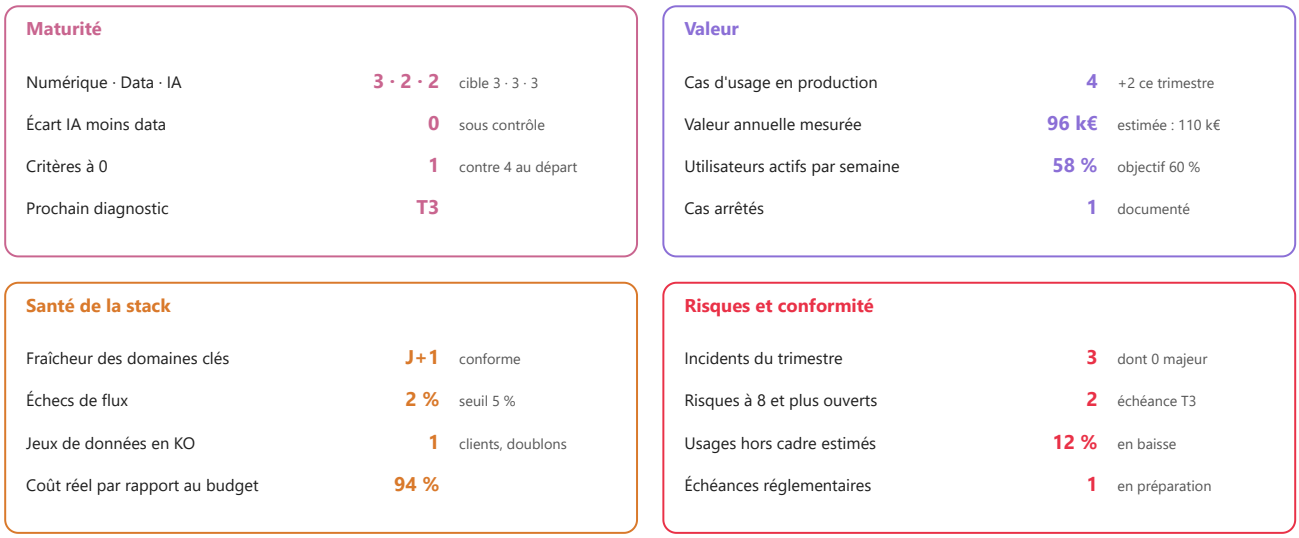
Le calendrier de la vie de la stack

Rythme	Ce qu'on fait	Qui
En continu	Alertes de qualité, de fraîcheur et de coûts ; signalement des incidents	Responsable technique
Mensuel	Matrice de qualité, échantillon de conversations d'agents, suivi des coûts, veille (nouveaux modèles, alertes de sécurité, réglementation)	Intendants, responsable technique
Trimestriel	Comité : tableau de bord, portefeuille, risques, composants ; test de substitution des agents critiques	Comité
Semestriel	Diagnostic de maturité, matrice des contrôles par couche, revue des accès, test de restauration	Pilote du programme
Annuel	Charte, feuille de route, budget, bilan de la valeur	Comité, direction

Les signes qu'une stack se fige. Plus personne ne sait pourquoi tel outil a été choisi. Un composant n'a pas été revu depuis un an. Le comité ne s'est pas réuni depuis deux trimestres. Les agents se multiplient sans que personne ne regarde leur inventaire. La solution n'est pas technique : il faut reprendre les rituels.

10.2 Le tableau de bord de pilotage

Une seule page, qui ouvre chaque comité. Quatre blocs, trois ou quatre indicateurs par bloc, avec leur tendance. Les chiffres ci-dessous sont inventés pour l'exemple.



Exemple fictif de tableau de bord trimestriel.

10.3 À l'échelle : gouvernance fédérée et produits de données

Au niveau 4, ou dans une ETI répartie sur plusieurs sites, un comité central unique devient vite un goulet d'étranglement. Le modèle s'adapte, sans changer de principes.

- **Un comité central** fixe les règles, les choix structurants et le budget. **Des comités de domaine** (une direction, une filiale) gèrent leurs propres cas d'usage.
- **Des produits de données par domaine.** Chaque domaine publie ses jeux de données avec un propriétaire, une définition, un niveau de qualité et des conditions d'accès. C'est l'esprit du data mesh.
- **Des standards communs** (couche sémantique, classification, connecteurs), tenus au niveau central, pour que les domaines restent compatibles entre eux.

Règles du tableau de bord

- **Peu d'indicateurs** : seize au plus, quatre par bloc. Au-delà, plus personne ne les lit.
- **Toujours un point de comparaison** : une cible, un seuil, ou le trimestre précédent.
- **Les mêmes définitions** que la couche sémantique. Le tableau de bord du comité doit montrer l'exemple.
- **Une décision par alerte.** Tout indicateur hors seuil donne lieu à une décision ou à une action, notée au relevé.

→ *Gabarit 11.20*

Partie 11. *Toutes les matrices et tous les gabarits du guide vous attendent dans la boîte à outils, prêts à imprimer et à remplir.*

PARTIE 11 · BOÎTE À OUTILS

11.1 Matrice de maturité

MATRICE · 2 PAGES

Mode d'emploi. Pour chaque critère, cochez la description la plus proche de la réalité, preuve à l'appui. Les niveaux 1 et 3 se situent entre les descriptions voisines. Calculez ensuite la note de chaque axe (moyenne arrondie à l'inférieur, plafonnée à 2 si un critère est à 0) et reportez-la sur le radar de la page suivante.

Axe numérique

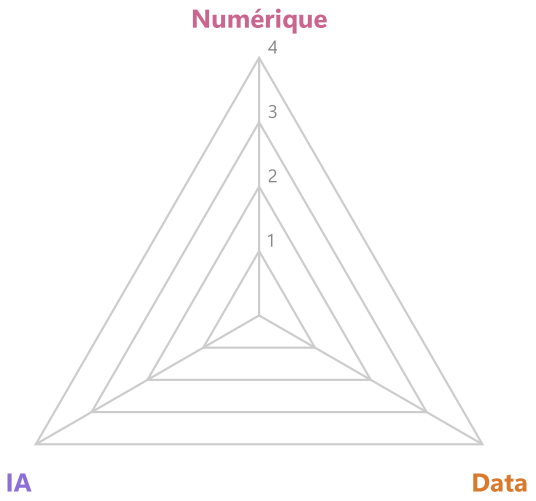
Critère	Niveau 0	Niveau 2	Niveau 4	Note
N1. Processus	Papier, messagerie	Processus clés dématérialisés	Tous les processus numériques de bout en bout	
N2. Applications	Tableurs isolés	ERP ou CRM sur les fonctions clés	Toutes les fonctions outillées	
N3. Intégration	Ressaisies	Exports et imports manuels	API et flux automatiques	
N4. Identité	Comptes partagés	Comptes nominatifs par outil	Identité unique (SSO), revue des accès	
N5. Hébergement, sécurité	Non maîtrisés	Sauvegardes, antivirus, règles de base	Politique de sécurité, cloud maîtrisé, tests	
N6. Compétences	Usage minimal	Formation aux outils métier	Culture numérique, référents par service	
			Note de l'axe numérique	

Axe data

Critère	Niveau 0	Niveau 2	Niveau 4	Note
D1. Accès	Extractions à la demande	Exports réguliers	Accès automatique à toutes les sources	
D2. Centralisation	Aucune	Socle sur quelques domaines	Socle commun à toute l'entreprise	
D3. Définitions	Implicites	Partielles, documentées	Toutes versionnées, une seule par indicateur	
D4. Propriétaires	Personne	Quelques domaines	Chaque jeu de données	
D5. Qualité	Non mesurée	Contrôles ponctuels	Tests automatiques, seuils, alertes	
D6. Décision	À l'intuition	Tableaux de bord consultés	Décisions documentées par les données	
			Note de l'axe data	

Axe IA

Critère	Niveau 0	Niveau 2	Niveau 4	Note
I1. Usages connus	Inconnus	Recensés	Tous au registre, suivis	
I2. Cadre	Aucun	Outil choisi, charte diffusée	Cadre appliqué et contrôlé	
I3. Compétences	Aucune formation	Formation de base	Référents, parcours par métier	
I4. Intégration	Outils isolés	Assistants sur les documents	Agents connectés aux données et au SI	
I5. Gouvernance	Aucune	Règles RGPD appliquées	Registre, AI Act, revue trimestrielle	
I6. Valeur	Non mesurée	Estimée par cas d'usage	Mesurée et pilotée	
			Note de l'axe IA	



Radar à compléter : tracez le triangle actuel en trait plein, la cible en pointillés.

Synthèse	Actuel	Cible
Numérique		
Data		
IA		
Écart IA − data		

Date du diagnostic : ..... Participants : .....

Conditions organisationnelles

Sponsor nommé à la direction	☐ oui	Ambition data et IA écrite	☐ oui
Budget dédié	☐ oui	Temps réservé pour les équipes	☐ oui

Trois constats à retenir

1.
2.
3.

Critères à 0 à traiter en priorité

PARTIE 11 · BOÎTE À OUTILS

11.2 Matrice de priorisation

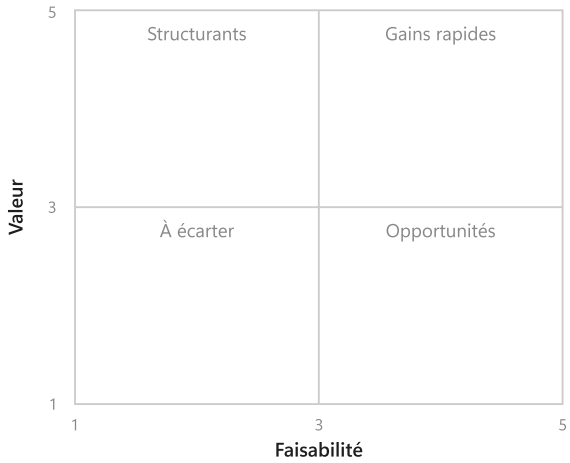
MATRICE · 1 PAGE

Mode d'emploi. Notez chaque cas d'usage de 1 à 5 en valeur et en faisabilité à l'aide des repères ci-dessous, puis qualifiez le risque. Reportez chaque cas sur la matrice. Le score (valeur × faisabilité) départage les cas d'une même zone. Un risque élevé ne se compense pas par un bon score : il impose un avis du référent conformité.

Note	Valeur	Faisabilité
1	Gain marginal, peu de personnes concernées	Prérequis absents, données inexistantes
3	Gain réel sur une équipe, estimable	Un prérequis à combler, données partielles
5	Gain fort, chiffré, sur plusieurs équipes	Réalisable tout de suite, sponsor disponible

Risque : **faible** (données publiques ou internes, erreur sans conséquence) · **moyen** (données confidentielles, erreur corrigible) · **élevé** (données personnelles, décision sur des personnes, action irréversible, catégorie sensible de l'AI Act).

#	Cas d'usage	Valeur	Faisabilité	Score	Risque	Zone	Décision
Ex.	*Synthèse des comptes rendus de réunion*	*4*	*5*	*20*	*Faible*	*Gain rapide*	*Lancer*
Ex.	*Prévision des stocks*	*5*	*2*	*10*	*Moyen*	*Structurant*	*Socle stock d'abord*
1							
2							
3							
4							
5							
6							



Portefeuille retenu

Gain rapide sans socle data	
Projet structurant	
Autres cas retenus	
Domaines du socle minimal	

PARTIE 11 · BOÎTE À OUTILS

11.3 Matrice des prérequis

MATRICE · 1 PAGE

Mode d'emploi. Listez vos cas d'usage d'IA envisagés. Pour chacun, indiquez la famille d'usage (voir 2.4), les niveaux requis, puis vos niveaux actuels issus de la matrice 11.1. Un écart positif signifie que le cas d'usage n'est pas réaliste en l'état : il faut soit attendre, soit réduire son ambition, soit financer la montée en maturité correspondante.

Cas d'usage envisagé	Famille d'usage	Numérique		Data		Décision
		Requis	Actuel	Requis	Actuel	
Exemple : assistant qui répond aux commerciaux sur les ventes du mois	*Questions sur les chiffres*	*2*	*3*	*3*	*1*	*Reporter ; inclure les ventes dans le socle minimal*
Exemple : synthèse automatique des comptes rendus de réunion	*Productivité individuelle*	*1*	*3*	*0*	*1*	*Lancer avec la charte*

Les cas d'usage retenus passent ensuite dans la matrice de priorisation (11.2), qui ajoute la valeur et le risque.

PARTIE 11 · BOÎTE À OUTILS

11.4 Matrice RACI

MATRICE · 1 PAGE

Mode d'emploi. Adaptez les colonnes aux rôles réels de l'entreprise, puis remplissez chaque case avec R (réalise), A (approuve et répond), C (consulté) ou I (informé). Vérifiez qu'il y a un seul A par ligne et au moins un R. Ajoutez vos propres activités dans les lignes vides. Un exemple rempli figure en 8.4.

Activité	Comité	Propriétaire de données	Intendant	Resp. technique	Réf. conformité	Utilisateurs
Fixer l'ambition et le budget						
Proposer un cas d'usage						
Évaluer et prioriser un cas d'usage						
Valider un cas en voie rapide						
Définir ou modifier un indicateur						
Ouvrir un accès à des données						
Choisir ou remplacer un outil						
Mettre un agent en production						
Valider une action irréversible d'un agent						
Traiter un incident IA						
Répondre à une demande d'effacement						
Former les utilisateurs						
Conduire la revue trimestrielle						

Contrôles

Chaque ligne a un seul A	☐
Chaque ligne a au moins un R	☐
Aucun rôle n'est A sur plus de la moitié des lignes (risque d'engorgement)	☐
Chaque rôle est attribué à une personne nommée	☐

Validé par le comité le : ..... Prochaine revue : .....

PARTIE 11 · BOÎTE À OUTILS

11.5 Matrice de classification des données

MATRICE · 1 PAGE

Mode d'emploi. Les quatre classes et les règles proposées en 8.3 servent de point de départ. Adaptez-les, puis complétez les exemples propres à l'entreprise. La matrice est validée par le DPO et la DSI, puis diffusée avec la charte.

Classe	Définition	Exemples dans l'entreprise	Modèles autorisés	Agents autorisés
Public	Information déjà publiée ou publiable sans dommage		Tous ceux de la liste blanche	Tous
Interne	Réservée aux salariés, dommage limité en cas de fuite		Sous contrat, sans entraînement	Agents internes
Confidentiel	Accès restreint, dommage important en cas de fuite		Sous contrat, rétention minimale, UE de préférence	Espaces restreints
Personnel	Données relatives à une personne identifiable		Hébergés UE ou données pseudonymisées	Cas validé par le DPO

Règles complémentaires

Règle	Décision de l'entreprise
Qui attribue la classe d'un jeu de données ?	
Classe par défaut d'un document non marqué	
Marquage des documents (en-tête, métadonnées, dossier)	
Durée de conservation par classe	
Revue de la classification	

Validée le : ..... par : .....

PARTIE 11 · BOÎTE À OUTILS

11.6 Matrice de choix d'outils

MATRICE · 1 PAGE

Mode d'emploi. Fixez les poids avant de rencontrer les fournisseurs (total 100) ; adaptez-les à la case (5.3). Notez chaque candidat de 1 à 5 sur chaque critère, après l'essai sur vos données. Le score pondéré est la note multipliée par le poids. Un critère éliminatoire non satisfait (localisation, contrat, sécurité) écarte le candidat quel que soit son score.

Case concernée : ..... Cas d'usage visés : .....

Critère	Poids	Candidat A :		Candidat B :		Candidat C :	
		Note	Pondéré	Note	Pondéré	Note	Pondéré
Adéquation au besoin	20						
Intégration	15						
Sécurité et conformité	15						
Coût total sur trois ans	15						
Réversibilité	10						
Exploitabilité	10						
Solidité du fournisseur	10						
Ouverture (modèles, MCP)	5						
Total	100						

Critères éliminatoires

Exigence	A	B	C
Données traitées dans la zone exigée	☐	☐	☐
Pas de réutilisation des données pour l'entraînement	☐	☐	☐
Contrat de sous-traitance conforme	☐	☐	☐
Connexion par l'identité unique de l'entreprise	☐	☐	☐
Export complet des données et configurations	☐	☐	☐

Décision et plan de sortie

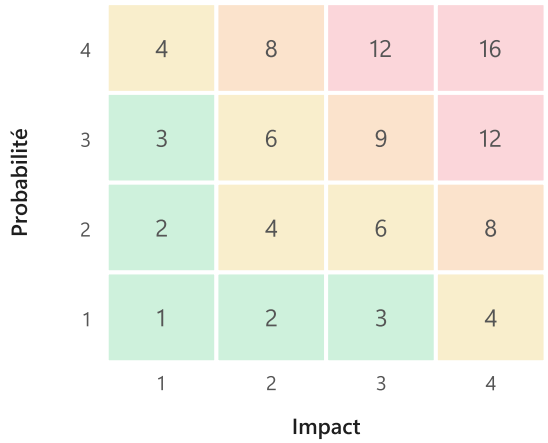
Candidat retenu et motif	
Plan de sortie (export, délai, coût estimé)	
Date de revue du choix	

PARTIE 11 · BOÎTE À OUTILS

11.7 Matrice des risques IA

MATRICE · 1 PAGE

Mode d'emploi. Pour chaque cas d'usage en pilote ou en production, listez les risques à partir des dix menaces de la partie 6.4. Notez la probabilité et l'impact de 1 à 4, calculez la criticité (probabilité × impact) et placez le risque sur la carte. Tout risque de criticité 8 ou plus doit avoir une mesure, un responsable et une échéance avant la mise en production. La matrice est revue chaque trimestre.



Note	Probabilité	Impact
1	Improbable	Gêne interne, sans suite
2	Possible	Erreur corrigible, coût limité
3	Probable	Client touché, coût significatif
4	Quasi certain	Fuite de données, sanction, atteinte à l'image

Vert : accepter et surveiller · jaune : réduire · orange : réduire avant production · rouge : ne pas mettre en production.

Cas d'usage	Risque (menace n°)	P	I	Crit.	Mesures	Responsable	Échéance
Assistant courriels clients	*Injection d'instructions (1)*	*3*	*3*	*9*	*Pas d'accès aux données financières ; validation humaine avant envoi*	*Resp. technique*	*Avant pilote*
Questions sur les ventes	*Fuite par l'agent (2)*	*2*	*3*	*6*	*Droits hérités ; espaces par équipe*	*Resp. technique*	*Avant pilote*

Date de revue : ..... Validé par : .....

PARTIE 11 · BOÎTE À OUTILS

11.8 Matrice des contrôles par couche

MATRICE · 1 PAGE

Mode d'emploi. Pour chaque couche, vérifiez que le contrôle attendu (8.2) est en place, nommez son responsable et indiquez la preuve (document, configuration, journal). Un contrôle absent devient une action datée. La matrice est revue chaque semestre.

Couche	Contrôle attendu	En place	Responsable	Preuve
Sources	Propriétaire nommé, classification à la source, base légale identifiée	☐		
Ingestion	Lignage et journal des chargements, aucune logique métier	☐		
Socle	Accès par zone, durée de conservation et purge, hébergement UE	☐		
Couche sémantique	Une métrique = une définition = un responsable	☐		
Restitution	Tableaux de bord certifiés distingués des exploratoires	☐		
Connaissance	Circuit de publication, date de revue sur chaque contenu	☐		
Agents	Droits hérités, identité et superviseur par agent, journal d'usage	☐		
Modèles	Liste blanche, données autorisées selon la classe, contrats	☐		
Orchestration	Validation humaine sur l'irréversible, traçabilité	☐		
Transversal	SSO, revue des accès, incidents, plan de sortie	☐		

Actions

Contrôle manquant	Action	Responsable	Échéance

Revue du : ..... Prochaine revue : .....

PARTIE 11 · BOÎTE À OUTILS

11.9 Matrice de qualité des données

MATRICE · 1 PAGE

Mode d'emploi. Listez les jeux de données critiques (ceux des cas d'usage prioritaires). Pour chaque dimension utile, inscrivez le seuil fixé avec le propriétaire, puis l'état constaté : **OK**, **À surveiller** ou **KO**. Une dimension sans objet reste vide. Mettez la matrice à jour chaque mois et présentez-la au comité chaque trimestre.

Jeu de données	Propriétaire	Exactitude	Complétude	Unicité	Fraîcheur	Cohérence	Validité	Action
Clients	*Dir. commerciale*		*Région < 2 % vide · OK*	*Doublons < 1 % · KO*	*J+1 · OK*	*ERP = CRM · À surv.*	*OK*	*Dédoublonnage dans l'ERP*

Synthèse du mois

Jeux de données en KO	
Agents ou tableaux de bord concernés	
Corrections à la source engagées	

Mise à jour par : ..... Date : .....

PARTIE 11 · BOÎTE À OUTILS

11.10 Grille de diagnostic de l'existant

GABARIT · 2 PAGES

Mode d'emploi. Pour chaque couche du modèle (partie 3), décrivez l'existant (outils, état, qui s'en occupe) et la cible à 18 mois. Notez l'écart de 0 (aucun) à 3 (tout à construire) et la priorité de 1 (immédiate) à 3 (plus tard), en fonction des cas d'usage retenus. Une couche qu'aucun cas d'usage prioritaire ne réclame reste en priorité 3, même si l'écart est grand.

Couche	Existant	Cible à 18 mois	Écart 0-3	Priorité 1-3	Propriétaire
Ex. : 4. Couche sémantique	*Indicateurs calculés dans des tableurs, définitions différentes selon les services*	*20 indicateurs définis, versionnés, un responsable chacun*	*3*	*1*	*Direction financière*
1. Sources					
2. Ingestion					
3. Socle de données					
4. Couche sémantique					
5. Restitution					
6. Connaissance					
7. Agents					
8. Modèles					
9. Orchestration					
Transversal : identité, sécurité					
Transversal : conformité, coûts					

Synthèse

Couches en priorité 1	
Principaux risques identifiés	
Dépendances fortes à un fournisseur	

Inventaire des usages d'IA existants

Recensez les usages réels, y compris ceux qui ne passent pas par des outils approuvés. Le questionnaire est anonyme : l'objectif est de connaître les besoins, pas de sanctionner.

Outil	Service	Utilisateurs	Usage	Données saisies	Classe	Décision
Assistant grand public, comptes personnels	*Commercial*	*8*	*Rédaction de propositions*	*Noms de clients, prix*	*Confid.*	*Remplacer par l'outil approuvé*

Décisions possibles : garder (outil approuvé, usage conforme) · remplacer (besoin réel, outil ou données non conformes) · arrêter (usage exclu par la charte).

Besoins exprimés et idées de cas d'usage

Diagnostic réalisé par : ..... Période : .....

PARTIE 11 · BOÎTE À OUTILS

11.11 Fiche cas d'usage

GABARIT · 1 PAGE

Mode d'emploi. Une fiche par cas d'usage, remplie par le propriétaire du cas d'usage avec l'appui de l'équipe technique. Elle sert à l'évaluation (étape 2 du cycle de vie), puis devient la référence du registre des cas d'usage.

Identification	
Nom du cas d'usage	
Fonction et équipe concernées	
Propriétaire du cas d'usage	
Le besoin	
Problème à résoudre aujourd'hui	
Ce que fera l'IA, concrètement	
Ce qui reste une décision humaine	
La valeur	
Valeur attendue (chiffrée)	
Situation de référence à mesurer	
Indicateurs de succès et seuil	
Nombre d'utilisateurs visés	
Les données et le système	
Données et documents utilisés	
Classe des données (public, interne, confidentiel, personnel)	
Logiciels concernés, lecture ou écriture	
Famille d'usage et prérequis (11.3)	
Le risque	
Conséquence d'une erreur	
Niveau d'autonomie visé (A1 à A4, 6.4)	
Niveau de risque (faible, moyen, élevé)	
Catégorie AI Act et avis conformité	
L'évaluation	
Valeur (1-5) · Faisabilité (1-5) · Score	
Éligible à la voie rapide (4.4) ?	
Décision du comité et date	
Durée du pilote et date de revue	

PARTIE 11 · BOÎTE À OUTILS

11.12 Registre des cas d'usage

GABARIT · 1 PAGE

Mode d'emploi. Une ligne par cas d'usage, quel que soit son statut : proposé, en évaluation, en pilote, en production, arrêté. Le registre est tenu par le propriétaire de données désigné (8.1) et examiné à chaque revue trimestrielle. Un cas arrêté reste inscrit, avec ce qu'il a appris.

ID	Cas d'usage	Propriétaire	Étape	Valeur estimée / mesurée	Risque	Classe	AI Act	Coût annuel	Revue	Statut
UC-01	*Synthèse des comptes rendus*	*Dir. des opérations*	*5*	*24 k€ / 21 k€*	*Faible*	*Interne*	*Minimal*	*6 k€*	*T3*	*Production*

Étapes : 1 proposition · 2 évaluation · 3 pilote · 4 revue · 5 production (4.4). Ajouter « VR » au statut d'un cas validé en voie rapide.

PARTIE 11 · BOÎTE À OUTILS

11.13 Registre des composants

GABARIT · 1 PAGE

Mode d'emploi. Une ligne par case du modèle occupée par un outil. Le registre est tenu par le responsable technique. Il sert à la revue des composants, au suivi des coûts et à la réversibilité : chaque ligne indique comment sortir de l'outil.

Case	Occupant	Type	Coût annuel	Contrat, échéance	Données, localisation	Responsable	Plan de sortie	Revue	Note 11.6
3. Socle	*Entrepôt cloud*	*Managé*	*4 k€*	*Mensuel, sans engagement*	*Interne, confid. ; UE*	*Resp. technique*	*Export des tables en format ouvert, 2 semaines*	*T4*	*4,1*

Type : managé · auto-hébergé · mixte. Une case sans occupant n'apparaît pas : elle n'est ajoutée qu'à la demande d'un cas d'usage (règle de sobriété, 3.5). Chaque agent en production y figure aussi : identité dans « Occupant », superviseur dans « Responsable », niveau d'autonomie (A1 à A4) et outils accessibles dans « Données, localisation » (6.4).

PARTIE 11 · BOÎTE À OUTILS

11.14 Glossaire des indicateurs

GABARIT · 1 PAGE

Mode d'emploi. Une ligne par indicateur utilisé dans plus d'un tableau de bord ou par un agent. La définition métier est rédigée par le propriétaire ; la règle de calcul est écrite avec l'intendant. Toute modification crée une nouvelle version, datée. Les agents et les tableaux de bord ne lisent que les indicateurs inscrits ici.

Indicateur	Définition métier	Règle de calcul	Source	Responsable	Version	Utilisé par
Chiffre d'affaires net	*Ventes facturées, hors taxes, déduction faite des avoirs*	*Somme des lignes de facture HT moins avoirs, par date de facture*	*marts_ventes*	*Dir. financière*	*v2, 03/2026*	*Tableau CODIR, agent ventes*
Client actif	*Client ayant passé au moins une commande sur douze mois glissants*	*Clients distincts avec commande dans les 365 derniers jours*	*marts_clients*	*Dir. commerciale*	*v1, 01/2026*	*Tableau commercial*

PARTIE 11 · BOÎTE À OUTILS

11.15 Check-list de mise en production d'un agent

GABARIT · 1 PAGE

Mode d'emploi. À remplir par le responsable technique avec le propriétaire du cas d'usage, avant toute mise en production et à chaque changement majeur. Tout point non coché est justifié dans la colonne commentaire et accepté explicitement par le comité.

Agent : ..... Version : ..... Date : .....

Point de contrôle	Fait	Commentaire
Cas d'usage		
Fiche cas d'usage complète (11.11) et validée par le comité	☐	
Propriétaire nommé	☐	
Situation de référence mesurée	☐	
Données et droits		
Classe des données identifiée et compatible avec le modèle utilisé	☐	
Droits hérités de l'utilisateur, testés avec plusieurs profils	☐	
Lecture de la couche sémantique ou de marts_, jamais du brut	☐	
Sécurité		
Principe des trois capacités respecté	☐	
Tests d'injection passés	☐	
Connecteurs et serveurs MCP approuvés uniquement, droits minimaux par outil	☐	
Comptes de service au moindre privilège, secrets en coffre	☐	
Qualité des réponses		
Jeu de test constitué et validé par le métier	☐	
Seuils d'exactitude atteints	☐	
Sources citées dans les réponses	☐	
Refus appropriés hors périmètre ; test de substitution sur un second modèle (agents critiques)	☐	
Contrôle humain		
Validation humaine sur toute action irréversible	☐	
Plafonds définis (montants, volumes)	☐	
Coupure de l'agent possible en quelques minutes ; identité propre et superviseur nommé ; niveau d'autonomie (A1 à A4) fixé (6.4)	☐	
Conformité		
Qualification AI Act faite (8.5)	☐	
Registre des traitements à jour, analyse d'impact si nécessaire	☐	
Personnes informées lorsqu'elles échangent avec une IA	☐	
Exploitation		
Journal des échanges et des actions actif	☐	
Supervision et alertes en place	☐	
Quotas et suivi des coûts configurés	☐	
Utilisateurs formés, contact de signalement connu	☐	

Responsable technique :	Propriétaire du cas d'usage :

PARTIE 11 · BOÎTE À OUTILS

11.16 Modèle de charte d'usage de l'IA

GABARIT · 1 PAGE

Modèle à adapter. Les passages entre crochets sont à compléter. À faire valider par le DPO, la DSI, les RH et, le cas échéant, à présenter aux représentants du personnel.

1. Objet

La présente charte encadre l'usage des outils d'intelligence artificielle par les collaborateurs de [entreprise], afin d'en tirer parti tout en protégeant les données, les clients et les personnes.

2. Outils autorisés

Seuls les outils suivants peuvent être utilisés avec des données de l'entreprise : [liste]. Ils sont accessibles via [accès]. Tout autre outil ne peut être utilisé qu'avec des informations publiques.

3. Données

Il est interdit de saisir dans un outil d'IA des données [personnelles / confidentielles] hors des outils et des cas d'usage approuvés pour ces classes de données. Exemples interdits : [fichier clients, données salariés, conditions commerciales, codes d'accès].

4. Vérification et responsabilité

L'utilisateur vérifie tout contenu produit avec l'IA avant de l'utiliser ou de le diffuser. Il reste responsable du résultat. L'IA ne prend aucune décision sur une personne sans intervention humaine.

5. Transparence

Un contenu diffusé à l'extérieur et produit en grande partie par l'IA est signalé lorsque [règle]. Les clients sont informés lorsqu'ils échangent avec un agent conversationnel.

6. Usages exclus

Sont exclus : les usages interdits par la loi, le contournement des règles de sécurité, l'évaluation de personnes hors des processus approuvés, la soumission de contenus protégés de tiers sans droit.

7. Formation

L'accès aux outils est ouvert après la formation [nom, durée]. Une mise à jour est proposée [fréquence].

8. Signalement

Tout doute, erreur ou incident est signalé à [contact], sans délai. Un signalement de bonne foi n'expose à aucune sanction.

9. Révision

La charte est revue chaque année par le comité data et IA. Version [n°] du [date].

Lu et accepté, nom :	Date et signature :

PARTIE 11 · BOÎTE À OUTILS

11.17 Cahier des charges pour consulter un fournisseur

GABARIT · 1 PAGE

Mode d'emploi. À envoyer à trois fournisseurs au plus (5.3). Les questions de sécurité et de conformité reprennent la partie 8.7 ; les critères d'évaluation, la matrice 11.6. Joindre la fiche des cas d'usage visés (11.11), sans données réelles.

1. Contexte et besoin	
Présentation de l'entreprise (activité, taille, outils en place)	
Case du modèle concernée et cas d'usage visés	
Volumes (utilisateurs, données, requêtes)	
2. Exigences	
Fonctionnalités attendues	
Intégrations requises (sources, SSO, API, connecteurs MCP)	
Localisation et souveraineté	
Sécurité (certifications, chiffrement, journalisation)	
Conformité (contrat de sous-traitance, non-réutilisation des données, AI Act)	
Réversibilité (export, formats, délai)	
3. Modalités	
Essai sur nos données : durée, périmètre, conditions	
Critères d'évaluation et pondération (11.6)	
Éléments de réponse attendus (prix sur trois ans, références comparables, feuille de route)	
Calendrier (questions, réponse, essai, décision)	
Contact et modalités de réponse	

PARTIE 11 · BOÎTE À OUTILS

11.18 Fiche de décision CODIR

GABARIT · 1 PAGE

Mode d'emploi. Une fiche par décision soumise au CODIR ou au comité : choix structurant, budget, lancement ou arrêt d'un cas d'usage, choix d'outil. Elle tient sur une page et se lit en cinq minutes. La recommandation est séparée des options, pour que la discussion porte sur des faits.

Décision demandée (une phrase)	
Contexte (trois lignes au plus)	
Lien avec la feuille de route et le profil de maturité	

Options	Coût	Valeur attendue	Risques	Délai
A.				
B.				
C. Ne rien faire				

Recommandation et motif	
Décision prise	
Conditions, jalons, indicateurs de suivi	
Responsable de la mise en œuvre	
Date de revue de la décision	

Présentée par : ..... Date : ..... Décision n° : .....

PARTIE 11 · BOÎTE À OUTILS

11.19 Gabarit de budget

GABARIT · 2 PAGES

Mode d'emploi. Remplissez un exemplaire par scénario étudié (voir 9.6). Montants hors taxes. Valorisez le temps interne en équivalents temps plein (ETP) multipliés par un coût moyen chargé. Notez pour chaque ligne l'hypothèse retenue (nombre d'utilisateurs, volumes, devis) : c'est elle que le CODIR discutera.
Scénario étudié : .....

Poste	Construction	Fonct. an 1	Fonct. an 2	Fonct. an 3	Hypothèse
Abonnements					
Plateforme d'agents ou assistant					
BI et restitution					
Ingestion des données					
Orchestration					
Autres licences					
Consommation					
Modèles (appels directs)					
Entrepôt de données					
Hébergement					
Prestations					
Cadrage et diagnostic					
Intégration et socle data					
Développement des cas d'usage					
Juridique et conformité					
Temps interne (en ETP valorisés)					
Responsable data ou référent					
Équipe technique					
Métiers (ateliers, pilotes)					
DPO et gouvernance					
Accompagnement					
Formation					
Conduite du changement					
Total					

Valeur et retour sur investissement

	An 1	An 2	An 3	Cumul
Gains estimés (temps réemployé, revenus, coûts évités)				
Coûts totaux (construction + fonctionnement)				
Solde (gains − coûts)				
Retour sur investissement ((gains − coûts) ÷ coûts)				

Répartition par cas d'usage

Cas d'usage	Coût de fonct. annuel	Valeur annuelle estimée	Valeur ÷ coût	Quota mensuel	Décision
Ex. : synthèse des comptes rendus	*6 k€*	*24 k€*	*4*	*300 €*	*Poursuivre*
Socle data (mutualisé)		Financé comme investissement, réparti sur l'ensemble des cas d'usage			

Hypothèses, risques et points de décision

Rubrique	À compléter
Hypothèses structurantes (utilisateurs, volumes, adoption)	
Principaux risques budgétaires (consommation, dépassement, dépendance)	
Coût de sortie estimé des composants principaux	
Financements ou aides mobilisables	
Jalons de décision (poursuite, ajustement, arrêt)	

Établi par : ..... Date : ..... Présenté au CODIR le : .....

PARTIE 11 · BOÎTE À OUTILS

11.20 Tableau de bord de pilotage

GABARIT · 1 PAGE

Mode d'emploi. À remplir avant chaque comité (10.2). Quatre blocs, trois ou quatre indicateurs chacun, toujours avec une référence (cible, seuil ou trimestre précédent). Tendance : en hausse, stable, en baisse.

Trimestre : ..... Établi par : .....

Maturité

Indicateur	Valeur	Référence	Tendance

Valeur

Indicateur	Valeur	Référence	Tendance

Santé de la stack

Indicateur	Valeur	Référence	Tendance

Risques et conformité

Indicateur	Valeur	Référence	Tendance

Alertes et décisions proposées

Indicateur hors seuil	Analyse	Décision proposée

PARTIE 11 · BOÎTE À OUTILS

11.21 Ordre du jour de la revue trimestrielle

GABARIT · 1 PAGE

Mode d'emploi. Une réunion de 90 minutes au plus. Les documents sont envoyés une semaine avant : tableau de bord (11.20), registre des cas d'usage (11.12), matrice des risques (11.7), registre des composants (11.13). La réunion sert à décider, pas à découvrir les chiffres.

Date : ..... Participants : sponsor, pilote du programme, propriétaires de données, responsable technique, référent conformité, ...

#	Point	Durée	Porteur
1	Tableau de bord : maturité, valeur, santé, risques	15 min	Pilote du programme
2	Portefeuille : cas d'usage à lancer, ajuster, arrêter ou industrialiser ; cas validés en voie rapide (pour information)	30 min	Propriétaires
3	Risques et incidents du trimestre	15 min	Responsable technique
4	Composants et coûts : revues prévues, remplacements, test de substitution des agents critiques	10 min	Responsable technique
5	Conformité et évolutions réglementaires	10 min	Référent conformité
6	Relevé des décisions et des actions	10 min	Sponsor

Relevé de décisions

#	Décision	Responsable	Échéance

Points reportés au prochain comité

ANNEXES

A.1 Glossaire

Terme	Définition
A2A	Protocole de dialogue entre agents, complémentaire de MCP.
Agent	Programme d'IA qui, à partir d'une demande, enchaîne des étapes : chercher une information, appeler un outil, proposer ou déclencher une action.
AI Act	Règlement européen sur l'intelligence artificielle, qui encadre les systèmes d'IA selon leur niveau de risque.
AIPD	Analyse d'impact relative à la protection des données, exigée par le RGPD pour les traitements à risque élevé.
API	Interface qui permet à deux logiciels d'échanger des données de façon automatique.
Assistant	Outil d'IA qui répond à un utilisateur, sans agir de lui-même dans les logiciels.
Cas d'usage	Usage précis de la data ou de l'IA, avec un besoin, une valeur attendue et un responsable.
Couche sémantique	Couche qui définit une fois pour toutes les indicateurs (chiffre d'affaires, client actif) et que lisent tableaux de bord et agents.
Déployeur	Au sens de l'AI Act, organisation qui utilise un système d'IA sous sa propre autorité.
Données de référence	Données partagées entre logiciels (clients, produits, fournisseurs), pour lesquelles un système fait foi.
DPO	Délégué à la protection des données, référent RGPD de l'organisation.
ELT	Extraire, charger, transformer : on copie les données brutes dans le socle avant de les transformer.
Embeddings	Représentation d'un texte sous forme de nombres, qui permet de retrouver des passages proches par le sens.
Entrepôt de données	Base centrale où sont rassemblées et organisées les données des différents logiciels.
ETP	Équivalent temps plein.
FinOps	Pratique de pilotage des coûts des services en ligne et de l'IA.
Fournisseur	Au sens de l'AI Act, organisation qui développe un système d'IA et le met sur le marché.
Index vectoriel	Base qui stocke les embeddings pour la recherche par le sens.
Injection d'instructions	Attaque qui cache une consigne dans un contenu lu par l'IA pour détourner son comportement.
Intendant de données	Personne chargée de la qualité, du glossaire et du catalogue d'un domaine de données.
Lignage	Traçabilité du parcours d'une donnée, de la source jusqu'à l'indicateur.
marts_	Zone du socle qui contient les données modélisées, prêtes pour les usages métier.
MCP	Model Context Protocol : standard ouvert qui relie un agent à des outils et à des sources de données ; géré depuis fin 2025 par une fondation de la Linux Foundation.
Modèle (de langage)	Moteur d'IA qui comprend et produit du texte ; il est appelé par les assistants et les agents.
Niveau d'autonomie	Échelle de A1 (répondre) à A4 (agir seul dans des limites) qui fixe ce qu'un agent peut faire et les contrôles associés.
Orchestration	Enchaînement automatique d'actions entre plusieurs logiciels.
Passerelle de modèles	Point d'accès unique aux modèles, qui centralise les clés, les quotas et les journaux.
Pseudonymisation	Remplacement des données directement identifiantes par des codes, la correspondance étant conservée à part.
RACI	Répartition des rôles : réalise, approuve, consulté, informé.
Recherche augmentée	Technique qui fournit au modèle les passages pertinents d'une base documentaire avant qu'il réponde.
Registre des traitements	Document exigé par le RGPD qui recense les traitements de données personnelles.
Réponse inventée	Réponse fausse présentée avec assurance par une IA, parfois appelée hallucination.
RGPD	Règlement général sur la protection des données.
Shadow IA	Usage d'outils d'IA non approuvés par l'entreprise, souvent avec des comptes personnels.
Socle de données	Ensemble formé par l'entrepôt et ses zones (brut, nettoyé, métier).
SSO	Connexion unique : un seul identifiant donne accès à tous les outils de l'entreprise.
Stack	Ensemble des briques techniques qui collectent, stockent, définissent, restituent et exploitent les données.
Superviseur d'agent	Personne nommée qui répond du comportement d'un agent, valide ses évolutions et peut le couper.
Test de substitution	Rejouer le jeu de test d'un agent sur un autre modèle pour mesurer la dépendance à un fournisseur.
Voie rapide	Validation en continu d'un cas d'usage à faible risque, sans attendre le comité.
Webhook	Message envoyé automatiquement par un logiciel quand un événement se produit.

ANNEXES

A.2 Panorama des outils du marché

Exemples par catégorie, repris de la partie 5. Ils ne constituent pas des recommandations. Les offres, prix et positionnements évoluent vite : la consolidation du marché a été forte en 2026 (rachats, fusions, changements de nom). Chaque ligne a été vérifiée en novembre 2026 et doit l'être de nouveau à chaque édition.

Catégorie	Exemples	Vérifié le	Remarque
Hébergement	OVHcloud (UE), Scaleway (UE), Outscale (UE), régions UE des grands fournisseurs américains	11/2026	OVHcloud et Outscale ont des offres qualifiées SecNumCloud ; Scaleway en cours de qualification (automne 2026) ; vérifier la gamme exacte
Ingestion	Airbyte, Fivetran, dlt (UE)	11/2026	Fivetran a fusionné avec dbt Labs (juin 2026)
Socle de données	BigQuery, Snowflake, Postgres, ClickHouse	11/2026	Pas de changement majeur relevé
Transformation	dbt, SQLMesh	11/2026	dbt et SQLMesh appartiennent désormais au même groupe que Fivetran : attention à la dépendance
Couche sémantique	dbt Semantic Layer, Cube, Lightdash	11/2026	dbt Semantic Layer : même groupe que Fivetran
Restitution et BI	Data Studio (ex-Looker Studio), Metabase, Power BI, Lightdash	11/2026	Looker Studio renommé Data Studio en avril 2026
Connaissance	Strapi, Notion, Google Drive	11/2026	Pas de changement majeur relevé
Recherche sémantique	pgvector, Qdrant (UE), Weaviate (UE)	11/2026	Pas de changement majeur relevé
Plateforme d'agents	Dust (UE), Copilot Studio, Langdock (UE)	11/2026	Tarification par utilisateur, parfois par crédits : comparer à usage égal
Modèles	Claude, GPT, Mistral (UE), Gemini	11/2026	Versions renouvelées plusieurs fois par an : raisonner en familles
Connecteurs d\'agents	Serveurs MCP (standard ouvert), protocole A2A	11/2026	MCP confié à l\'Agentic AI Foundation (Linux Foundation) en décembre 2025
Passerelle de modèles	LiteLLM, OpenRouter	11/2026	OpenRouter racheté par Stripe en 2026 : préférer une passerelle open source maîtrisée pour rester neutre
Orchestration métier	n8n (UE), Make (UE), Zapier	11/2026	n8n : licence « fair-code », auto-hébergement possible pour un usage interne, pas open source au sens strict
Orchestration des pipelines	Dagster, Airflow, Kestra	11/2026	Airflow 2 en fin de vie depuis avril 2026 ; rachat de Dagster par Prefect annoncé en juillet 2026
Identité	SSO de la suite bureautique, Okta	11/2026	Pas de changement majeur relevé
Observabilité	Langfuse, Elementary	11/2026	Langfuse racheté par ClickHouse (janvier 2026), Elementary par Boomi (octobre 2026) ; projets open source maintenus

Liste non exhaustive. L'absence d'un outil ne signifie pas qu'il est déconseillé. (UE) : éditeur établi dans l'Union européenne.

ANNEXES

A.3 Hypothèses et limites

- **Guide neutre** : il ne recommande aucun fournisseur. Les outils cités illustrent des catégories.
- **Chiffres indicatifs** : budgets, durées, effectifs et seuils sont des ordres de grandeur proposés par le guide, à confronter à des devis et à la situation de chaque entreprise. Hypothèses de taille : environ 50 utilisateurs en PME, 300 en ETI.
- **Statistiques** : le guide ne cite que des études primaires vérifiées (Bpifrance Le Lab 2025, Gartner 2026). Les chiffres de baromètres connus seulement par des synthèses secondaires ont été écartés.
- **Réglementation** : les repères sur le RGPD, l'AI Act et les autres textes ont été vérifiés en novembre 2026, y compris le règlement modificatif (UE) 2026/1744. Ils doivent être revus à chaque édition. Ce guide ne constitue pas un avis juridique.
- **Contexte français** : certaines mentions (CSE, autorité de contrôle) visent la France ; elles sont à adapter dans d'autres pays.
- **Modèle de maturité** : l'échelle de 0 à 4, la règle du maillon faible et la règle des prérequis sont des propositions du guide, non une norme.

ANNEXES

A.4 Sources et références

Références vérifiées en novembre 2026.

Textes réglementaires

- Règlement (UE) 2016/679 relatif à la protection des données (RGPD), notamment les articles 5, 22, 28, 30, 33 et 35.
- Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act), notamment les articles 4, 5, 25, 26 et 50 et l'annexe III.
- Règlement (UE) 2026/1744 du 8 juillet 2026 (omnibus numérique sur l'IA), publié au JOUE le 24 juillet 2026, en vigueur le 27 juillet 2026 : report des obligations sur le haut risque, nouvelle rédaction de l'article 4.
- Directive (UE) 2022/2555 (NIS 2) et sa transposition nationale.
- Règlement (UE) 2023/2854 sur les données (Data Act), notamment l'article 29 sur les frais de changement de fournisseur cloud.
- Code du travail, article L. 2312-8 (information et consultation du CSE sur l'introduction de nouvelles technologies) ; tribunal judiciaire de Nanterre, 14 février 2025, n° 24/01457.

Lignes directrices et recommandations

- Commission européenne : lignes directrices sur les pratiques d'IA interdites et sur la définition d'un système d'IA.
- CNIL : recommandations et fiches pratiques sur l'IA et la protection des données.
- ANSSI : référentiel de qualification SecNumCloud.
- ANSSI : « Recommandations de sécurité pour un système d'IA générative », 29 avril 2024 (35 recommandations).
- OWASP : Top 10 for LLM Applications, édition 2025 (injection d'instructions, agentivité excessive, consommation non bornée, etc.) ; Non-Human Identities Top 10 (inventaire, droits et secrets des identités techniques).

Études et normes

- Bpifrance Le Lab, « L'IA dans les PME et ETI françaises : une révolution tranquille », juin 2025.
- Gartner, « Organizations with Successful AI Initiatives Invest Up to Four Times More in Data and Analytics Foundations », 16 avril 2026.
- ISO/IEC 42001:2023, système de management de l'intelligence artificielle ; NIST AI Risk Management Framework.
- CIGREF, ISACA France, IFACI : MAGNum 2026, modèle de maturité de la gouvernance du numérique.
- Model Context Protocol (Agentic AI Foundation) ; Open Semantic Interchange ; Apache Iceberg.
- IMDA (Singapour), Model AI Governance Framework for Agentic AI, janvier 2026 ; CNIL et CIANum, note sur l'IA agentique et les données personnelles, 20 juillet 2026.
- Commission européenne : stratégie Apply AI (8 octobre 2025) ; proposition de Cloud and AI Development Act, COM(2026) 502, 3 juin 2026.

Notions citées

- Simon Willison, « The lethal trifecta for AI agents », 16 juin 2025 (principe des trois capacités, 6.4).

Points vérifiés

Affirmation du guide	Source retenue	Vérifié le
Calendrier d'application de l'AI Act (8.5)	Règlement (UE) 2026/1744, art. 113 modifié de l'AI Act	11/2026
Recrutement classé à haut risque (4.2, 8.5)	AI Act, annexe III, point 4	11/2026
Notification des violations sous 72 heures (8.8)	RGPD, art. 33 ; CNIL	11/2026
Fourchettes budgétaires (9.6)	Tarifs publics des fournisseurs, recoupés partiellement ; construction non vérifiable	11/2026
Exemples d'outils (5.1, A.2)	Toutes les catégories de A.2 : sites des éditeurs, annonces de rachat, presse spécialisée	11/2026
Réversibilité et changement de fournisseur cloud (8.7)	Data Act, article 29	11/2026