

Du pilote à l'entreprise

Pourquoi l'IA réussit service par service, échoue à l'échelle de l'entreprise, et comment changer cela



Du pilote à l'entreprise

Pourquoi l'IA réussit service par service,
échoue à l'échelle de l'entreprise,
et comment changer cela

Un livre blanc outil pour les directions générales,
les comités de direction et les comités exécutif

Du pilote à l'entreprise

Un livre blanc U-CIE · Première édition, octobre 2026

État du droit et des sources vérifié au 25 octobre 2026

© 2026 u-cie.com, tous droits réservés.

Ce livre blanc est une œuvre protégée par le Code de la propriété intellectuelle. Son texte, sa structure, ses schémas, ses tableaux et ses outils (notamment la carte des trois flux, les quatre niveaux d'autonomie et le permis d'autonomie) sont la propriété de U-CIE.COM.

Ce que vous pouvez faire. Vous pouvez lire ce document, le transmettre gratuitement et dans son intégralité, et l'imprimer pour un usage interne à votre organisation. Vous pouvez reproduire et remplir les outils de la boîte à outils pour vos propres travaux internes. Vous pouvez en citer de courts extraits, à condition d'en indiquer clairement la source : « U-CIE, *Du pilote à l'entreprise*, 2026 ».

Ce qui nécessite notre accord écrit. Toute autre reproduction, représentation, adaptation ou traduction, totale ou partielle, par quelque procédé que ce soit, est soumise à l'autorisation préalable écrite de U-CIE.COM. Cela vaut notamment pour :

- la revente du document ;
- son utilisation dans une formation ou une prestation de conseil facturées ;
- la reprise de la méthode ou des outils sous un autre nom ;
- leur intégration dans un logiciel.

Toute reproduction non autorisée constitue une contrefaçon, sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Marques. U-CIE est une marque de UNNAMED COMPANY SAS

Sources tierces. Les travaux, rapports et textes cités appartiennent à leurs auteurs et éditeurs respectifs. Ils sont mentionnés à titre de référence, avec leur source, et leur citation n'implique aucune approbation de ce document par ces organismes.

Cas fictifs. Les entreprises, personnes et situations décrites dans ce livre blanc sont fictives. Toute ressemblance avec des organisations ou des personnes existantes serait fortuite. Elles ne décrivent ni des clients ni des missions de U-CIE.

Avertissement. Ce document propose un cadre de méthode et de gouvernance. Il ne constitue ni un avis juridique, ni une recommandation adaptée à une situation particulière. Les informations réglementaires reflètent l'état du droit au 25 octobre 2026 et peuvent évoluer. Avant toute décision, faites qualifier vos usages par vos conseils.

Crédits. Illustration de couverture : U-CIE. Conception et rédaction : U-CIE.

Éditeur. UNNAMED COMPANY SAS, 12 rue Vivienne - 75002 Paris. Directeur de la publication : Philippe Buschini

Sommaire

Mode d'emploi	5
L'essentiel en une page	6
Prologue : six mois dans la vie d'un pilote.....	7
Chapitre 1. Le malentendu : un pilote n'est pas une maquette réduite de l'entreprise	8
Ce qui protège un pilote, et disparaît à l'échelle	8
Deux erreurs symétriques	9
Chapitre 2. Changer de lunettes : voir l'entreprise en flux et en liaisons.....	10
Le flux, unité de mesure du dirigeant	10
Les six liaisons	10
Pourquoi le mot « intégration » est trompeur.....	11
Chapitre 3. Les effets en cascade : comment une petite erreur devient un gros problème	13
La bonne question n'est pas « peut-on faire confiance à l'IA ? ».....	14
Chapitre 4. Les agents : quand l'IA passe de conseiller à exécutant	15
Qu'est-ce qu'un agent, concrètement ?	15
Quatre points de vigilance	15
Le curseur d'autonomie : quatre niveaux	16
Chapitre 5. Ce que l'industrialisation change vraiment : sept chantiers	18
Chantier 1 : dessiner le flux avant de choisir l'outil	18
Chantier 2 : traiter la donnée comme un produit partagé.....	18
Chantier 3 : séparer la capacité de comprendre de la capacité d'agir	18
Chantier 4 : nommer qui décide de quoi.....	19
Chantier 5 : évaluer le système, pas seulement le modèle.....	19
Chantier 6 : former au flux, pas au prompt.....	20
Chantier 7 : gérer un portefeuille, pas une collection de prototypes	20
Chapitre 6. Le cadre européen, expliqué simplement.....	21
Le principe : on juge l'usage, pas la technologie.....	21
Le calendrier, vérifié au 25 octobre 2026	21

La maîtrise de l'IA : une obligation de moyens, déjà applicable	22
Le RGPD ne s'efface pas	22
Quand le déployeur devient fournisseur	23
Une méthode pragmatique.....	23
Chapitre 7. Cinq histoires fictives pour voir le mécanisme à l'œuvre	24
Hélianthe Exploitation : la maintenance qui semblait évidente	24
Signal Urbain : le compte rendu qui a perdu sa source.....	25
Club Partenaires Europe : l'agent commercial trop bien connecté	25
NordVale Finance : la frontière entre assistance et décision.....	26
Mécaforge Europe : la recommandation devenue ordre de production	26
Chapitre 8. Lire un budget d'industrialisation : ce que vous financez vraiment	28
Épilogue : revenir à la question de départ.....	30
Boîte à outils.....	31
Outil 1. Les dix questions avant de valider un passage à l'échelle	31
Outil 2. La carte des trois flux.....	31
Outil 3. Le permis d'autonomie.....	33
Outil 4. Les trois familles d'indicateurs de valeur	34
Outil 5. L'atelier de comité (2 h).....	34
Outil 6. Cinq signaux qu'un projet n'est pas prêt.....	35
Outil 7. Glossaire pour le comité.....	36
À propos de U-CIE.....	38
Références.....	39

Mode d'emploi

Ce document se lit comme une histoire et s'utilise comme une boîte à outils. Il a été pensé pour un comité de direction qui veut comprendre pourquoi ses projets d'IA calent au moment de grandir, puis décider quoi faire. Aucun bagage technique n'est nécessaire : chaque notion est expliquée la première fois qu'elle apparaît, et un glossaire figure dans la boîte à outils.

Le fil rouge suit un pilote d'IA au service client d'une entreprise fictive, de son succès en mars à ses difficultés en octobre. Chaque chapitre éclaire un mécanisme à partir de cette histoire, puis se termine par deux encadrés : **À retenir** fixe l'idée clé, **Pour votre comité** propose une question à poser lundi matin et l'outil qui permet d'y répondre.

Trois façons de s'en servir, selon le temps dont vous disposez :

Temps disponible	Ce qu'il faut lire	Ce que vous en retirez
5 minutes	« L'essentiel en une page »	Les six idées qui changent la façon de regarder un projet d'IA
20 minutes	Le prologue et les chapitres 1 à 5	Une grille de lecture pour challenger n'importe quel projet présenté en comité
Un atelier de 2 h	Les cas fictifs (chapitre 7), puis la boîte à outils, en fin de document	Une première cartographie de trois flux critiques de votre entreprise

Ce livre blanc forme une paire avec **Le curseur d'autonomie**, publié par U-CIE. Celui-ci explique pourquoi un projet d'IA tient ou casse au passage à l'échelle. Le second détaille comment décider, action par action, ce que l'IA a le droit de faire seule.

Un mot sur le statut des informations. Les règles juridiques citées ont été vérifiées au 25 octobre 2026. Les quatre niveaux d'autonomie et le permis d'autonomie sont une méthode de gouvernance proposée par U-CIE : ils ne figurent dans aucun texte de loi. Le document distingue toujours ce qui est obligatoire de ce qui est recommandé. L'histoire du prologue, les cinq cas sectoriels et toutes les entreprises mises en scène sont fictifs ; ils ne décrivent ni des clients ni des projets de U-CIE.

L'essentiel en une page

Si vous ne deviez retenir qu'une phrase : **l'IA ne bute presque jamais sur son intelligence, elle bute sur les coutures de l'entreprise.** Ces coutures, ce sont les données qui ne veulent pas dire la même chose d'un service à l'autre, les droits d'accès mal définis, les décisions dont personne ne sait qui les porte.

1. Un pilote réussi prouve une utilité, pas une capacité. Il montre qu'une équipe protégée, avec des données triées à la main et un expert à portée de voix, tire de la valeur d'un outil. Il ne dit encore rien de ce qui se passera avec dix équipes, cinq logiciels et des données qui changent tous les jours.

2. Votre entreprise n'est pas une addition de services, c'est un réseau de flux. Une commande devient livraison, puis facture, puis encaissement. C'est à ce niveau, celui du parcours complet, qu'il faut regarder ce que l'IA va modifier.

3. Entre deux étapes d'un flux, il y a toujours une liaison. Une donnée qui passe, un droit qui s'applique, une décision qui se prend, une responsabilité qui s'exerce. Brancher techniquement une IA ne règle aucune de ces liaisons.

4. L'IA accélère tout, y compris les erreurs. Là où un collaborateur expérimenté arrêterait sans y penser une information douteuse, un système rapide peut la faire voyager en quelques secondes jusqu'à une facture ou un client.

5. Les agents changent la nature du risque. Une IA qui suggère et une IA qui agit ne relèvent pas du même niveau de contrôle. L'autonomie se règle action par action, sur quatre niveaux (suggérer, préparer, exécuter, orchestrer), au rythme où l'on sait la surveiller et l'interrompre.

6. Industrialiser, c'est financer des liaisons, pas seulement des outils. Des données fiables, des droits bien bornés, des responsables nommés, des indicateurs posés avant le lancement. C'est moins spectaculaire qu'une démonstration, et c'est ce qui fait la différence.

La question qui résume tout le guide : **quels flux voulons-nous rendre plus capables grâce à l'IA, et quelles liaisons devons-nous renforcer pour que cette capacité reste digne de confiance à l'échelle ?**

Prologue : six mois dans la vie d'un pilote

Une histoire imaginaire, mais que beaucoup de comités de direction reconnaîtront. Nous y reviendrons tout au long du guide.

Mars. Au service client d'un groupe de services, une petite équipe teste un assistant d'IA. Un conseiller tape une question ; l'outil retrouve le contrat, résume l'historique du client et propose une réponse. En réunion de démonstration, l'effet est immédiat : ce qui prenait vingt minutes en prend cinq. La directrice du service veut aller plus loin.

Juin. Le comité de direction valide l'extension à trois autres entités. On achète des licences, on organise des formations. L'enthousiasme est général.

Septembre. Les premiers signaux faibles arrivent. Dans une filiale, « client actif » ne recouvre pas la même réalité que dans la maison mère, et l'assistant mélange les deux. Ailleurs, un conseiller découvre qu'il peut consulter des informations auxquelles il n'avait jamais eu accès. Une réponse impeccablement rédigée cite une clause qui n'existe plus depuis la dernière renégociation. Enfin, le logiciel de gestion change de version et une connexion cesse de fonctionner, sans que personne ne s'en aperçoive pendant dix jours.

Octobre. En comité, la question tombe : « le projet marche-t-il, oui ou non ? » Personne ne sait vraiment répondre. Les utilisateurs du pilote d'origine en sont toujours ravis. Les nouvelles entités, beaucoup moins.

Que s'est-il passé ? Le modèle d'IA n'est pas devenu moins bon entre mars et octobre. **C'est l'environnement qui a changé.** Au départ, une poignée de personnes compensaient sans le dire toutes les imperfections : elles triaient les documents, connaissaient les exceptions, rattrapaient les erreurs. À l'échelle, ces amortisseurs ont disparu, et les dépendances que le pilote masquait sont devenues visibles.

Voilà le paradoxe au cœur de ce guide. L'IA réussit souvent **service par service**, parce qu'un petit périmètre peut être protégé. Elle échoue **à l'échelle de l'entreprise** quand cette protection disparaît.

Pour comprendre pourquoi, il faut d'abord dissiper un malentendu sur ce qu'un pilote démontre vraiment.

Chapitre 1. Le malentendu : un pilote n'est pas une maquette réduite de l'entreprise

Un chef qui réussit un plat superbe pour six invités n'a pas encore prouvé qu'il peut servir trois cents couverts chaque soir. Pour cela, il lui faut une brigade, des fournisseurs réguliers, des recettes écrites, des normes d'hygiène et quelqu'un qui décide quand un plat repart en cuisine. Le talent est le même. Le système autour n'a rien à voir.

Un pilote d'IA, c'est le dîner pour six. Il répond à une vraie question, et c'est une bonne question : **dans des conditions choisies, l'IA aide-t-elle une équipe à mieux faire une tâche ?** Mais le comité de direction doit trancher une autre question : **l'entreprise peut-elle faire tourner cet usage de façon répétable, sûre et mesurable, avec plusieurs équipes, plusieurs logiciels, des données vivantes et des responsables identifiés ?** Ce ne sont pas deux étapes d'un même chemin, ce sont deux questions différentes, qui appellent deux types de preuves.

Ce qui protège un pilote, et disparaît à l'échelle

Reprenons l'assistant du prologue. En mars, tout jouait en sa faveur, souvent sans que personne s'en rende compte :

Dans le pilote	À l'échelle de l'entreprise
Un cas choisi parce qu'il est simple à comprendre	Des cas variés, dont certains très atypiques
Des documents triés et nettoyés à la main	Des données qu'il faut collecter, documenter et maintenir dans la durée
Un expert métier disponible à chaque étape	Des utilisateurs qui ne savent pas toujours qui appeler
Des volontaires déjà convaincus	Des populations hétérogènes, parfois sceptiques
Des exceptions rares, rattrapées par l'équipe projet	Des exceptions quotidiennes que personne n'a jamais décrites
Des erreurs sans grande conséquence	Des erreurs qui touchent un paiement, un client, un salarié

Ces protections ne sont pas une faute : elles permettent d'apprendre vite et à moindre risque. Le problème naît quand on oublie qu'elles existaient. L'OCDE observe d'ailleurs que les entreprises qui adoptent l'IA doivent souvent organiser la collecte systématique de données issues de leurs processus, et que la qualité, la structure et l'intégration de données hétérogènes restent des difficultés récurrentes [1].

Deux erreurs symétriques

La première erreur consiste à lire un pilote réussi comme une autorisation implicite de généraliser. La seconde, à conclure de difficultés d'industrialisation que le pilote ne valait rien. Dans les deux cas, on confond deux niveaux de décision.

Un pilote peut être excellent et son passage à l'échelle laborieux, parce que ce passage demande des investissements dans les processus, les données, les compétences et la gouvernance. Les économistes qui étudient les technologies dites « d'usage général », celles qui transforment toute l'économie comme l'a fait l'électricité, décrivent ce décalage : les gains n'apparaissent souvent qu'une fois l'organisation réinventée autour de la technologie [4].

C'est pourquoi le cadre de gestion des risques du NIST, l'institut américain de référence en matière de normes et de technologie, demande de documenter dès le départ la finalité du système, ses utilisateurs, ses contextes d'utilisation, ses limites et les compétences nécessaires pour l'exploiter [2] [3]. Il ne s'agit pas de paperasse : c'est ce qui transforme une démonstration en un système que l'entreprise comprend et dont elle peut rendre compte.

À retenir. Un pilote prouve qu'un usage est utile dans des conditions protégées. Il ne prouve pas que l'entreprise sait le faire fonctionner sans ces protections.

Pour votre comité. *Question à poser :* ce pilote nous a prouvé quoi, exactement, et qu'est-ce qu'il ne nous a pas encore prouvé ? *Outil :* les dix questions avant de valider un passage à l'échelle (boîte à outils, outil 1). Chaque case vide est un chantier à financer.

Si le pilote ne suffit pas à juger, il faut une autre façon de regarder l'entreprise.

Chapitre 2. Changer de lunettes : voir l'entreprise en flux et en liaisons

Dans un relais 4 × 100 mètres, une équipe perd rarement la course parce qu'un coureur est lent. Elle la perd au passage du témoin. Une entreprise fonctionne de la même manière : sa performance se joue autant dans les transmissions entre étapes que dans chaque étape elle-même. Or c'est précisément là, dans les transmissions, que l'IA vient s'insérer.

Le flux, unité de mesure du dirigeant

Un **flux**, dans ce guide, c'est l'enchaînement complet qui transforme un déclencheur en résultat métier. Pas la procédure écrite : ce qui se passe vraiment, avec les fichiers envoyés par courriel, les vérifications informelles, les ressaisies, les coups de téléphone et les raccourcis que les équipes ont inventés pour que le travail avance.

Prenez une réclamation client, comme celles que traitait l'assistant du prologue. Le flux commence quand le message arrive et se termine quand le client a obtenu satisfaction. Entre les deux, quelqu'un identifie le client, retrouve son contrat, évalue l'urgence, choisit un interlocuteur, propose une solution, consigne l'action, puis ferme ou rouvre le dossier. L'IA peut intervenir à presque chaque étape : trier le message, retrouver une clause, résumer l'historique, rédiger une réponse, préparer une mise à jour dans le CRM (le logiciel qui centralise la relation client).

À chacun de ces endroits, elle dépend de ce que nous appelons des **liaisons** : ce qui permet à une étape de recevoir l'information, le droit ou la décision dont la suivante a besoin. On peut les ranger en six familles.

Les six liaisons

Liaison	En clair	La question qui la révèle
Données	L'information est-elle juste, à jour, et veut-elle dire la même chose partout ?	« Qu'appelle-t-on exactement un client actif, et quel logiciel fait foi ? »
Applications	La façon dont l'IA se branche sur vos logiciels (CRM, comptabilité, messagerie, planification)	« Si cette connexion tombe, qui s'en aperçoit, et en combien de temps ? »
Identité et droits	Au nom de qui l'IA agit, et à quoi elle a accès	« Peut-elle voir ou faire ce que l'utilisateur lui-même n'a pas le droit de faire ? »

Liaison	En clair	La question qui la révèle
Décision	Ce que l'IA fait de son résultat : suggérer, préparer, exécuter ou orchestrer (chapitre 4)	« Qui tranche, et selon quelle règle, quand le cas sort de l'ordinaire ? »
Responsabilité	Qui détecte, corrige, suspend, prévient	« Qui a le droit d'appuyer sur le bouton d'arrêt ? »
Mesure	Comment on sait que le flux s'améliore vraiment	« Quel chiffre de départ avions-nous, et que regardons-nous chaque mois ? »

Relisez le mois de septembre du prologue avec ce tableau en tête : chaque incident correspond à une liaison. La définition de « client actif » relève des **données**. Le conseiller qui voit trop d'informations, des **droits**. La connexion cassée pendant dix jours, des **applications** et de la **responsabilité** : personne n'était chargé de la surveiller. Et l'impossibilité de dire en octobre si le projet marche relève de la **mesure**.

Quelques repères issus des travaux de référence permettent d'aller plus loin. Sur les données, connecter deux logiciels ne suffit pas s'ils ne parlent pas le même langage métier : une étude du Centre commun de recherche de la Commission européenne montre que cette couche « de sens », dite sémantique, est déterminante dans la plupart des cas étudiés [5].

Sur les droits, les spécialistes de la sécurité recommandent que l'IA agisse toujours dans le contexte de l'utilisateur concerné, avec le minimum d'accès nécessaire, et que ce soient les logiciels eux-mêmes qui vérifient les autorisations, pas le modèle d'IA [6] [7]. Sur la responsabilité, le NIST organise la gestion des risques autour de quatre fonctions (gouverner, cartographier, mesurer, gérer) et attend des rôles clairs, un inventaire des systèmes et un engagement explicite de la direction [2]. Sur la mesure, il recommande de comparer en continu les résultats observés en conditions réelles avec ceux obtenus pendant les tests [8].

Pourquoi le mot « intégration » est trompeur

On parle volontiers « d'intégrer » l'IA au système d'information. Le mot évoque un câble que l'on branche. Or passer à l'échelle demande aussi d'intégrer du sens, de l'autorité, du contrôle et de la responsabilité. Une IA peut être techniquement reliée à dix logiciels et rester inutilisable dans un flux critique si personne ne sait quelle donnée prévaut, qui valide, comment l'exception se traite, ni à quel moment on arrête tout.

À retenir. Regardez les projets d'IA à l'échelle du flux complet, et examinez chacune des six liaisons. Un projet bien branché techniquement peut rester fragile sur toutes les autres.

Pour votre comité. *Question à poser :* pour ce projet, pouvez-vous me montrer les six liaisons, et me dire lesquelles sont encore marquées « inconnu » ? *Outil :* la carte des trois flux (boîte à outils, outil 2).

Une liaison fragile n'est pas un problème isolé : elle devient le point de départ d'une réaction en chaîne.

Chapitre 3. Les effets en cascade : comment une petite erreur devient un gros problème

Dans un flux traité à la main, vos collaborateurs jouent un rôle qu'on ne voit pas : ce sont des disjoncteurs. Ils repèrent le chiffre bizarre dans un tableau, reconnaissent le client sensible, savent qu'un statut affiché dans le logiciel ne reflète pas la réalité du terrain. Cette expertise est précieuse, mais elle est rarement écrite nulle part.

L'IA met ces disjoncteurs à l'épreuve, parce qu'elle fait passer une information d'une étape à l'autre en quelques secondes : elle résume une note et alimente un ticket, lit un document et prépare un ordre dans un autre logiciel. Bien encadrée, cette vitesse crée beaucoup de valeur. Sans point d'arrêt, elle fait voyager les erreurs plus vite et plus loin. On appelle cela un **effet en cascade** : le résultat produit à une étape devient l'entrée, la décision ou l'action de l'étape suivante, et une erreur de départ se propage en gagnant de l'ampleur.

Ces cascades prennent cinq formes, qui correspondent aux liaisons du chapitre précédent.

La cascade de données. Une référence client est erronée dans un fichier source. L'IA la reprend, la reformule proprement sans signaler de doute, puis un autre logiciel rattache la demande au mauvais compte. L'IA n'a rien « inventé » : elle a fidèlement transmis une donnée fautive. Mais parce que l'outil passe pour fiable, l'erreur gagne en crédibilité à chaque étape.

La cascade de décision. L'IA classe une demande comme non prioritaire parce que certains mots attendus n'y figurent pas. Le manager, confiant, affecte la ressource ailleurs. Le délai s'allonge, le client se plaint plus haut. Aucun composant n'est « en panne » : c'est l'enchaînement entre une recommandation, une confiance excessive et une décision d'affectation qui produit le dégât.

La cascade de droits. Un assistant a reçu le droit de chercher dans une base documentaire, d'écrire dans le CRM et d'envoyer des courriels, le tout sous une seule identité aux accès très larges. Il suffit alors d'une consigne ambiguë, ou malveillante, pour déclencher une action qui dépasse largement le besoin. Le cas le plus connu s'appelle l'**injection d'instructions** (en anglais *prompt injection*). Imaginez un assistant de direction qui exécuterait toutes les consignes trouvées dans le courrier, y compris un post-it glissé par un inconnu dans une enveloppe. C'est ce qui peut arriver lorsqu'une IA lit un document ou un courriel contenant des instructions cachées : elle risque de les suivre comme si elles venaient de vous. Le NIST explique que, dans ces systèmes, la frontière entre « données à lire » et « ordres à exécuter » devient peu fiable [9]. L'OWASP, référence mondiale en sécurité des applications, cite parmi les conséquences possibles la fuite d'informations et le déclenchement d'actions non autorisées dans les systèmes connectés [6].

La cascade de confiance. Une réponse est bien écrite, structurée, convaincante. L'utilisateur relâche sa vigilance. Le texte est copié dans une note, la note dans un compte rendu, le compte rendu nourrit une décision. Le NIST parle de **confabulation** pour désigner la production assurée d'un contenu faux, et rappelle que même les sources et les explications citées par l'IA peuvent être erronées [10]. Le vrai danger n'est pas la réponse fausse : c'est la réponse fausse assez crédible pour franchir plusieurs contrôles. La clause périmée citée par l'assistant du prologue en est un exemple typique.

La cascade de responsabilité. Le métier a choisi l'outil, l'informatique a configuré la connexion, l'éditeur héberge le modèle, la sécurité gère les accès, le juridique a relu le contrat, les opérations utilisent le résultat. Chacun voit un morceau. Personne ne possède le flux de bout en bout, ni le droit de l'arrêter. Le projet semble bien gouverné, car il a beaucoup d'interlocuteurs ; il est en réalité fragile, car il n'a pas de propriétaire.

La bonne question n'est pas « peut-on faire confiance à l'IA ? »

Posée ainsi, la question n'appelle qu'une réponse vague, et oppose artificiellement l'humain et la machine. La question utile est plus précise : **dans ce flux, à quels résultats de l'IA accordons-nous quelle confiance, pour déclencher quelle action, sous quel contrôle et avec quel recours ?** Elle oblige à séparer ce qui est sans conséquence de ce qui touche un droit, une somme d'argent, une relation client, une consigne de sécurité ou une décision concernant une personne.

À retenir. L'IA ne crée pas seulement des erreurs nouvelles ; elle accélère et amplifie les erreurs existantes. Il faut savoir où se trouvent les points d'arrêt, avant que la cascade ne démarre.

Pour votre comité. *Question à poser :* si l'IA se trompe à la première étape, jusqu'où l'erreur peut-elle aller avant que quelqu'un ou quelque chose l'arrête ? *Outil :* la ligne « Jusqu'où une erreur ou un abus pourrait se propager » de la carte des trois flux (outil 2), jouée en simulation pendant l'atelier (outil 5, étape 4).

Ce risque change de dimension lorsque l'IA ne se contente plus de produire du texte, mais agit directement dans vos systèmes.

Chapitre 4. Les agents : quand l'IA passe de conseiller à exécutant

Le premier jour, vous ne confiez pas à un nouveau collaborateur la carte bancaire de l'entreprise et le pouvoir de signer les contrats. Vous lui accordez des délégations progressives, en fonction de ce qu'il a démontré et de ce que vous savez contrôler. C'est exactement ainsi qu'il faut raisonner avec les agents d'IA.

Qu'est-ce qu'un agent, concrètement ?

Un assistant d'IA classique répond : il rédige, résume, cherche. Un **agent** va plus loin : il combine un modèle d'IA avec des outils et des accès qui lui permettent d'**agir** dans vos logiciels. Il peut rechercher une information, comparer, créer un ticket, préparer un courriel, réserver un créneau, modifier une priorité. Ce n'est donc pas son intelligence qui le rend autonome, ce sont les portes que l'entreprise lui ouvre.

Imaginez que l'assistant du prologue devienne un agent. Dans sa version prudente, il lit la demande, retrouve le contrat, résume les incidents passés et propose une réponse. Dans une version plus autonome, il crée lui-même le ticket, change sa priorité, réserve une intervention, prévient le client et clôt certaines demandes. Chaque ajout semble anodin. Mis bout à bout, ils transforment un outil d'aide à la rédaction en rouage opérationnel de votre entreprise.

Une précision juridique utile : le terme « agent » ne constitue pas une catégorie à part dans le droit européen. Les obligations dépendent du rôle de l'entreprise, de la finalité du système et du niveau de risque de l'usage, comme on le verra au chapitre 6 [11]. Mais sur le plan opérationnel, l'autonomie et l'accès aux outils rendent le comportement plus difficile à prévoir, à tester et à surveiller. C'est le constat de l'agence britannique de cybersécurité, le NCSC [12].

Quatre points de vigilance

Comprendre n'est pas avoir le droit. Un agent peut parfaitement saisir qu'un client demande un remboursement. Cela ne lui donne pas l'autorité de l'accorder. C'est le logiciel financier qui doit vérifier qui peut valider, dans quelle limite, pour quel client et avec quels justificatifs.

Tout ce que l'agent lit doit être considéré comme non fiable. Un courriel, une pièce jointe, une page web peuvent contenir des instructions piégées, comme le post-it du chapitre précédent. Le NCSC indiquait qu'il n'existait pas, au moment de son analyse, de parade infaillible contre l'injection d'instructions [19]. La réponse n'est donc pas d'interdire toute lecture de documents externes, mais de faire en sorte qu'aucun contenu lu ne puisse étendre les droits de l'agent.

La vitesse réduit le temps de réaction. Ce qui traversait plusieurs mains en une journée s'exécute en quelques secondes. Si la validation humaine n'a pas été prévue au bon endroit, c'est-à-dire avant l'action irréversible, elle arrive trop tard [12].

Il faut pouvoir débrancher. Un agent en production doit pouvoir être bridé, mis en pause, révoqué ou ramené à un état connu. Cela suppose de savoir quelle version, quelles consignes, quelles sources et quels accès il utilisait, et de conserver des **journaux**, c'est-à-dire un enregistrement de ce qu'il a reçu, produit et déclenché, erreurs comprises [7].

Le curseur d'autonomie : quatre niveaux

La manière la plus simple de piloter ces questions est de raisonner en niveaux, comme pour une délégation de pouvoir, et de les régler **action par action**, pas outil par outil : un même assistant peut suggérer pour un geste et exécuter pour un autre. Deux questions suffisent pour situer chaque geste : qui déclenche l'action, et qui choisit ce qui vient ensuite ? Ces quatre niveaux relèvent de la méthode U-CIE et ne correspondent à aucune catégorie du règlement européen sur l'IA.

Niveau	Ce que fait l'IA	Exemple	Condition pour y accéder
1. Suggérer	Elle éclaire une décision : synthèse, options, signalement	Résumer un dossier avant un rendez-vous	Un usage cadré, des sources vérifiables, des utilisateurs formés
2. Préparer	Elle produit un acte prêt à partir, qu'une personne valide avant exécution	Préremplir une relance dans le CRM, envoyée après relecture du commercial	Un valideur nommé, qui dispose du temps, des informations et de l'autorité pour relire vraiment
3. Exécuter	Elle réalise seule une opération dont le scénario est fixé à l'avance	Déplacer un rendez-vous dans des créneaux autorisés	Action bornée et réversible, erreurs détectables, journaux, alertes, retour arrière possible
4. Orchestrer	Elle choisit elle-même l'enchaînement de plusieurs opérations autorisées pour atteindre un objectif	Traiter un incident de bout en bout dans un périmètre défini	Options de l'agent explicitement limitées, surveillance réelle, repli testé, capacité d'arrêt

Deux nuances évitent les contresens. D'abord, une validation humaine n'est une protection que si elle est réelle : un valideur qui clique en quelques secondes sur quatre-vingts dossiers par jour ne contrôle plus rien. Dans certains cas, un niveau 3 bien encadré est plus sûr qu'un niveau 2 devenu machinal.

Ensuite, le niveau 4 n'est pas interdit par principe ; il exige simplement des preuves beaucoup plus fortes. Le NCSC recommande de commencer par des tâches étroitement délimitées et de n'élargir les accès qu'après une évaluation et une surveillance satisfaisantes [12].

Le NCSC propose aussi un test de bon sens que tout dirigeant peut s'approprier : **si l'organisation ne peut pas comprendre, surveiller ou contenir les actions d'un agent, celui-ci n'est pas prêt à être déployé** [12]. Il ne s'agit pas de prédire chaque phrase de l'IA, mais de savoir ce qu'elle peut faire, où l'observer, ce qui la limite et comment l'arrêter.

Ce réglage se formalise dans un **permis d'autonomie** : une autorisation écrite, datée et révocable, qui fixe pour une action précise ce que l'IA peut faire seule, ce qu'elle doit faire valider et ce qu'elle ne fera jamais. Le livre blanc **Le curseur d'autonomie** détaille la méthode complète.

À retenir. L'autonomie d'une IA se délègue comme un pouvoir de signature : action par action, avec des plafonds, et en fonction des preuves accumulées. Elle se retire aussi simplement qu'elle s'accorde.

Pour votre comité. *Question à poser* : à quel niveau se situe chaque geste de l'IA aujourd'hui, à quel niveau veut-on l'amener, et quelle preuve attendons-nous pour monter d'un cran ? *Outil* : le permis d'autonomie (boîte à outils, outil 3).

Nous savons maintenant ce qui fragilise un projet d'IA à l'échelle. Reste la question pratique : que faut-il construire pour le rendre solide ?

Chapitre 5. Ce que l'industrialisation change vraiment : sept chantiers

Industrialiser l'IA ne se résume pas à un projet, ni à une plateforme, ni à une charte éthique. C'est une capacité qui se construit par couches, un peu comme une maison : les beaux meubles ne servent à rien si les fondations, la plomberie et l'électricité ne suivent pas. Chacune des sept couches ci-dessous doit être à la hauteur des enjeux du flux concerné. Aucune ne remplace les autres.

Chantier 1 : dessiner le flux avant de choisir l'outil

Avant de décider ce que l'IA fera seule, il faut cartographier le résultat attendu, le déclencheur, les étapes, les données, les décisions, les exceptions et le point d'arrivée [3]. Cet exercice oblige à se poser des questions souvent absentes des démonstrations. Quelle étape crée le plus de retard ? Quelle décision est réellement difficile ? Quelle exception l'expert traite-t-il sans jamais l'écrire ? Et quel acte ne doit pas être confié à la machine, même si c'est techniquement possible ?

Chantier 2 : traiter la donnée comme un produit partagé

Une donnée qui compte pour un flux doit avoir une définition, un propriétaire, une origine connue, une règle de qualité et une fréquence de mise à jour, comme un produit qu'on livre à ses clients internes. Une IA peut produire une réponse brillante à partir de documents contradictoires. Elle ne peut pas décider seule quel référentiel fait foi : cette décision appartient à l'entreprise [5]. Le gouvernement britannique rappelle d'ailleurs que préparer des données pour l'IA ne se réduit jamais à une question de format : la qualité, le contexte, la sécurité et la conformité en font partie [13].

Chantier 3 : séparer la capacité de comprendre de la capacité d'agir

C'est sans doute le principe d'architecture le plus important de ce guide. L'IA peut interpréter une demande et préparer une intention. Mais ce sont les logiciels qui détiennent les données ou exécutent l'action qui doivent vérifier l'identité, le droit et les règles métier. Sinon, l'assistant devient de fait **un super-utilisateur déguisé en conversation** : un compte qui peut tout voir et tout faire, auquel on parle comme à un collègue.

Le principe du « moindre privilège » consiste à ne donner à chaque usage que les accès strictement nécessaires. Un agent qui propose des créneaux de rendez-vous n'a aucune raison d'accéder aux dossiers de rémunération. Des accès temporaires, limités à une action et tracés, valent souvent mieux que des autorisations permanentes accordées pour aller vite [7].

Chantier 4 : nommer qui décide de quoi

Inutile de créer une organisation lourde. Il faut en revanche que, pour chaque flux assisté par l'IA, on puisse remplir ce tableau sans hésiter. Une même personne peut tenir plusieurs rôles dans une entreprise de taille moyenne ; l'essentiel est qu'aucun ne reste vide.

Rôle	Ce qu'il porte
Propriétaire métier	Le résultat attendu et la valeur créée ; il porte le permis d'autonomie
Responsable du processus	Le déroulé du flux, ses étapes et ses exceptions
Responsable des données	La qualité, la définition et la mise à jour des référentiels
Responsable technique	L'exploitation, les connexions, la surveillance
Risque et conformité	L'analyse, proportionnée au niveau d'exposition
Détenteur du droit d'arrêt	La décision de suspendre, de redémarrer ou de faire évoluer le système

Le NIST ne prescrit pas d'organigramme type, mais il demande des rôles documentés et place la responsabilité des décisions de risque au niveau de la direction [2]. La norme internationale ISO/IEC 42001 propose, de son côté, un système de management de l'IA à l'échelle de l'organisation, dans une logique d'amélioration continue [16].

Chantier 5 : évaluer le système, pas seulement le modèle

Un modèle peut briller sur une série de questions-tests et échouer face à des documents incomplets, une demande ambiguë, une connexion coupée ou une règle qui a changé. Le NIST met en garde contre les conclusions tirées d'évaluations étroites ou anecdotiques [10]. Pour juger la **valeur** d'un usage, une évaluation utile regarde trois choses à la fois :

- **la qualité du résultat** : exactitude, complétude, sources traçables ;
- **la qualité du flux** : délais, reprises, escalades, erreurs détectées, charge reportée sur d'autres équipes ;
- **les conséquences** : impact client, financier, humain, réglementaire ou de sécurité.

Une réponse plus rapide n'améliore rien si elle génère deux fois plus de vérifications en aval. C'est souvent ce qui se cache derrière un gain de productivité annoncé mais introuvable dans les comptes. Pour décider ensuite d'accorder davantage d'**autonomie**, il faut en plus vérifier la maîtrise (le système

respecte-t-il ses limites et ses droits ?) et la résilience (que se passe-t-il en cas de changement, de panne ou d'attaque ?), comme le détaille *Le curseur d'autonomie*.

Chantier 6 : former au flux, pas au prompt

L'OCDE souligne que les compétences nécessaires dépassent largement l'expertise technique : il faut des bases numériques, des capacités transversales et un savoir-faire managérial pour décider ce qui revient à l'humain et ce qui peut revenir à la machine [17]. Concrètement, l'opérateur doit savoir reconnaître les limites de l'outil et signaler une anomalie ; le manager doit comprendre comment la performance est mesurée ; les fonctions de contrôle doivent pouvoir relire une trace exploitable. Les enquêtes de l'OCDE associent d'ailleurs la formation et la consultation des salariés à de meilleurs résultats pour eux [18].

Chantier 7 : gérer un portefeuille, pas une collection de prototypes

Tous les flux ne méritent pas le même investissement ni la même autonomie. Mieux vaut commencer là où la valeur, le risque, la maturité des données et la capacité de supervision sont alignés. Une tâche très rentable mais nourrie de données douteuses peut exiger d'abord un chantier de données. Une tâche réglementée peut demander un déploiement plus lent sans être pour autant un mauvais cas d'usage.

La maturité d'une entreprise ne se mesure donc pas au nombre de prototypes. Elle se mesure à sa capacité à arbitrer ces dépendances explicitement, puis à reproduire la méthode d'un flux à l'autre.

À retenir. L'industrialisation repose sur sept couches complémentaires : le flux, les données, les accès, les rôles, l'évaluation, les compétences et le portefeuille. La plus faible fixe le niveau d'autonomie possible.

Pour votre comité. *Question à poser :* sur ces sept chantiers, lesquels sont réellement couverts par le plan qu'on nous présente, et lesquels sont implicitement supposés réglés ? *Outil :* les cinq signaux qu'un projet n'est pas prêt (boîte à outils, outil 6).

Plusieurs de ces chantiers ont une dimension réglementaire. Avant de passer aux cas pratiques, il est utile de savoir ce que le droit européen exige, et à partir de quand.

Chapitre 6. Le cadre européen, expliqué simplement

La conformité n'est pas un tampon qu'on appose à la fin. Bien comprise, c'est une aide à la conception : elle oblige à se poser, au bon moment, les questions que ce guide recommande de toute façon.

Le principe : on juge l'usage, pas la technologie

Le règlement européen sur l'intelligence artificielle (souvent appelé *AI Act*) ne crée pas de catégorie juridique « IA agentique », et ne parle nulle part de niveaux d'autonomie. Il raisonne selon trois critères : **le rôle** de votre entreprise, **la finalité** du système et **le niveau de risque** de l'usage concret [11].

Sur le rôle, deux notions suffisent pour commencer. Le **fournisseur** est celui qui développe un système d'IA et le met sur le marché ou en service sous son nom. Le **déploieur** est l'organisation qui l'utilise dans son activité professionnelle. La plupart des entreprises sont déploiements de la plupart de leurs outils.

Conséquence très pratique : un même outil peut être anodin dans un usage et sensible dans un autre. Un assistant interne qui aide à rédiger n'est pas, par nature, un système à haut risque. Le même type d'outil utilisé pour trier des candidatures, évaluer des salariés ou apprécier la solvabilité de particuliers peut relever des usages à haut risque. Ces usages sont énumérés à l'annexe III du règlement, une liste de domaines jugés sensibles (emploi, crédit, éducation, accès aux services essentiels, entre autres) ; le classement dépend toujours de l'analyse précise de l'usage [11].

Le calendrier, vérifié au 25 octobre 2026

Le règlement (UE) 2026/1744, dit « omnibus numérique sur l'IA », est entré en vigueur le 27 juillet 2026. Il a repoussé les obligations les plus lourdes, celles des systèmes à haut risque, sans reporter l'ensemble du texte [22] [25].

Date	Ce qui s'applique	Statut au 25 octobre 2026
2 février 2025	Pratiques interdites, définitions, obligation de maîtrise de l'IA (article 4)	En vigueur
2 août 2025	Règles de gouvernance et obligations des fournisseurs de modèles d'IA à usage général	En vigueur
27 juillet 2026	Entrée en vigueur du règlement 2026/1744 ; réécriture de l'article 4	En vigueur
2 août 2026	Application générale du règlement, dont les obligations de	En vigueur

Date	Ce qui s'applique	Statut au 25 octobre 2026
	transparence (avec des délais transitoires pour certains systèmes déjà sur le marché)	
2 décembre 2027	Obligations des systèmes à haut risque de l'annexe III (emploi, crédit, éducation, accès aux services essentiels, etc.)	À venir (initialement prévu au 2 août 2026)
2 août 2028	Obligations des systèmes à haut risque intégrés à des produits réglementés (annexe I : machines, dispositifs médicaux, etc.)	À venir (initialement prévu au 2 août 2027)

Attention à l'effet d'optique du report. Il ne concerne que le régime des systèmes à haut risque. Le RGPD, les interdictions, la maîtrise de l'IA, la transparence et vos obligations générales de sécurité continuent de s'appliquer. Et un système RH qui devra être conforme en décembre 2027 se prépare dès maintenant : la mise en conformité implique des changements de processus qui ne s'improvisent pas en quelques semaines.

La maîtrise de l'IA : une obligation de moyens, déjà applicable

Depuis l'omnibus, l'article 4 ne demande plus de « garantir » un niveau suffisant de maîtrise de l'IA. Fournisseurs et déployeurs doivent **prendre des mesures pour favoriser son développement** auprès de leur personnel et des personnes qui utilisent les systèmes pour leur compte, sans être tenus de garantir un niveau déterminé pour chaque individu [22] [26]. En termes juridiques, on passe d'une obligation de résultat à une obligation de moyens : il faut pouvoir montrer qu'on a agi.

Pour une direction, l'enjeu pratique reste entier : il faut que chacun comprenne les capacités et les limites de l'outil dans son rôle, les règles d'usage, les risques de divulgation et la marche à suivre en cas de doute. C'est exactement le chantier 6 du chapitre précédent.

Le RGPD ne s'efface pas

Dès qu'un flux d'IA manipule des données personnelles, que ce soit dans les documents fournis, les consignes, les journaux ou les résultats, l'analyse RGPD reste nécessaire : base légale, finalité, minimisation, exactitude, durée de conservation, sécurité, sous-traitants, transferts hors de l'Union et, si besoin, analyse d'impact [20]. Deux pièges reviennent souvent :

- **pseudonymiser n'est pas anonymiser.** Remplacer un nom par un code ne rend pas une donnée anonyme si l'on peut encore remonter à la personne. Le Comité européen de la

protection des données rappelle que l'anonymat d'un modèle entraîné sur des données personnelles s'apprécie au cas par cas [21] ;

- **une décision entièrement automatisée** qui produit un effet juridique ou affecte significativement une personne est encadrée par l'article 22 du RGPD [20]. Faire intervenir un valideur ne suffit pas, à lui seul, à sortir de ce régime : son intervention doit être réelle.

Quand le déployeur devient fournisseur

Utiliser un modèle via le service d'un grand éditeur ne vous fait pas endosser toutes les obligations de cet éditeur. En revanche, si vous mettez en service sous votre nom un système à haut risque, si vous le modifiez substantiellement ou si vous changez sa finalité au point de le rendre à haut risque, vous pouvez hériter des obligations du fournisseur [11]. C'est un point à vérifier avant chaque élargissement d'usage, et l'une des raisons pour lesquelles un pilote anodin peut devenir, une fois étendu, un sujet de conformité.

Une méthode pragmatique

La CNIL recommande de partir d'un besoin concret, de définir les usages autorisés et interdits, de vérifier ce que le prestataire fait des données, de former les utilisateurs et d'associer dès le départ les métiers, les systèmes d'information, le responsable de la sécurité et le délégué à la protection des données [23]. C'est la logique même de ce guide.

À retenir. Le droit européen juge l'usage, pas l'outil. Le report du haut risque à fin 2027 ne suspend ni le RGPD, ni la maîtrise de l'IA, ni la transparence.

Avertissement. Ce livre blanc propose un cadre de gouvernance, pas un avis juridique. La qualification au regard du règlement sur l'IA, du RGPD ou des règles sectorielles dépend de l'usage réel, du rôle de l'organisation et du contexte.

Pour votre comité. *Question à poser :* pour cet usage, sommes-nous fournisseur ou déployeur, quelle est sa finalité exacte, et un élargissement prévu pourrait-il changer sa catégorie de risque ?
Outil : la dixième question de l'outil 1, croisée avec une première qualification juridique par vos conseils.

Les principes sont posés. Voyons maintenant comment ils se manifestent dans des situations concrètes.

Chapitre 7. Cinq histoires fictives pour voir le mécanisme à l'œuvre

Les entreprises ci-dessous sont fictives. Ces cas ne décrivent ni des clients ni des résultats de U-CIE. Ils montrent, dans cinq univers différents, comment les mêmes liaisons décident du succès ou de l'échec du passage à l'échelle. Chaque histoire suit le même déroulé : le pilote, le point de rupture, la leçon.

Cas	Secteur	Liaison qui casse	Leçon en une phrase
Hélianthe Exploitation	Énergies renouvelables	Données (définitions)	Un bon résumé ne dit pas quelle définition fait foi
Signal Urbain	Marketing terrain	Données (statut de l'information)	L'IA met en forme ; elle ne transforme pas une estimation en preuve
Club Partenaires Europe	Hospitalité sportive	Identité et droits	Préparer une offre n'est pas avoir le droit de l'engager
NordVale Finance	Crédit	Décision	Résumer un dossier n'est pas juger un dossier
Mécaforge Europe	Industrie	Décision et responsabilité	Une recommandation qualité ne doit pas devenir un ordre de production par glissement

Hélianthe Exploitation : la maintenance qui semblait évidente

Le pilote. Cet exploitant de parcs solaires et éoliens teste, sur un site, un assistant qui lit les comptes rendus de maintenance et en tire une synthèse : équipement concerné, anomalie, pièce évoquée, prochaine action possible. Un responsable relit tout. Rien ne part automatiquement vers la planification ni vers les achats. Les techniciens gagnent du temps.

Le point de rupture. Étendu à tous les parcs, l'outil révèle ce que le pilote cachait. Un même équipement porte trois codes différents selon le logiciel de supervision, celui de maintenance et celui des achats. Le mot « indisponibilité » n'est pas calculé de la même façon par l'exploitation, la maintenance et la finance. Les contrats de sous-traitance ne répartissent pas les responsabilités de la même manière. L'IA produit toujours d'excellents résumés, mais elle ne peut pas décider seule quelle définition prévaut, ni si une recommandation justifie un ordre de travail.

La leçon. Le vrai chantier devient le flux « de l'alerte à la remise en service » : une source de vérité pour chaque équipement, une règle de criticité, une personne qui valide, une méthode de mesure. Tant que ce flux n'est pas consolidé, l'IA reste aux niveaux 1 et 2. Le succès ne se juge plus au temps de rédaction gagné, mais à un délai de qualification réduit sans hausse des erreurs ni des réinterventions [8].

Signal Urbain : le compte rendu qui a perdu sa source

Le pilote. Cette agence de marketing terrain transforme les notes vocales de ses responsables terrain en comptes rendus de campagne, classés par lieu, créneau, volume de contacts et incidents. Chaque auteur relit son texte, l'usage reste interne : tout fonctionne.

Le point de rupture. L'agence relie l'outil à son CRM, à l'espace client et à la facturation. Soudain, le statut de chaque information compte. « Contact qualifié » ne veut pas dire la même chose pour le client, pour les commerciaux et pour le terrain. Les notes contiennent des appréciations, des photos, parfois des coordonnées. Une estimation faite à la volée sur le trottoir peut se retrouver dans un rapport client comme un chiffre ferme, simplement parce que l'IA l'a bien formulée.

La leçon. Il faut séparer les observations brutes, les indicateurs de gestion et ce qui peut être communiqué au client. Les chiffres contractuels viennent de sources identifiées, chaque publication a un responsable, et les données personnelles sont examinées au regard du RGPD [20]. L'IA accélère la mise en forme ; elle ne change pas une donnée incertaine en preuve.

Club Partenaires Europe : l'agent commercial trop bien connecté

Le pilote. Cette entreprise organise des prestations d'hospitalité autour de grands événements sportifs : loges, repas, accueil d'invités, logistique. Un assistant retrouve les échanges passés avec un client et propose une réponse, que le commercial relit, corrige et envoie lui-même. L'assistant ne touche ni aux réservations ni aux contrats. On est au niveau 1, puis au niveau 2 quand les propositions sont préremplies dans le CRM.

Le point de rupture. On veut relier l'outil à la réservation et à la facturation : vérifier une disponibilité, poser une option sur une loge, relancer le client. Or une offre dépend de la disponibilité, de clauses contractuelles, de conditions de paiement, et une option posée peut être facturée. Un accès trop large expose aussi des informations de négociation, et un courriel entrant piégé peut influencer un agent qui dispose d'outils pour agir.

La leçon. On dissocie quatre gestes : rechercher, recommander, préparer, exécuter. L'agent peut chercher et préparer. Le CRM, le système de réservation et l'outil financier vérifient l'identité, les disponibilités, les règles de prix et les plafonds d'engagement avant toute action [6]. Ce qui engage l'entreprise (offre ferme, option, remise, paiement) ne se délègue pas sans décision explicite du comité. Le livre blanc *Le curseur d'autonomie* suit cette entreprise pendant douze mois, permis par permis.

NordVale Finance : la frontière entre assistance et décision

Le pilote. L'équipe d'un établissement de crédit teste une IA qui résume les pièces d'un dossier de financement, signale les documents manquants et prépare une note pour l'analyste. Celui-ci garde l'accès aux sources, son jugement et la décision. L'outil fait gagner du temps de recherche, rien de plus.

Le point de rupture. L'extension vers le système de décision, les données externes et le parcours d'entrée en relation change complètement le cadre. L'évaluation de la solvabilité de particuliers figure parmi les usages à haut risque listés à l'annexe III du règlement sur l'IA, selon leur finalité concrète [11]. Une décision entièrement automatisée qui affecte significativement une personne est en outre encadrée par l'article 22 du RGPD [20].

La leçon. Il faut tenir la frontière entre synthèse, recommandation et décision. Pour la synthèse, on vérifie la fidélité aux pièces, la détection des manques, la traçabilité et la confidentialité. Pour une recommandation ou une décision, il faut rendre visibles les critères, les données utilisées, la supervision, l'explication et les voies de recours. Le raccourci dangereux serait de prendre un gain de temps sur la lecture comme justification pour automatiser le jugement.

Mécaforge Europe : la recommandation devenue ordre de production

Le pilote. Sur un site, une IA lit les non-conformités, l'historique de maintenance et les commentaires des opérateurs pour préparer les réunions qualité. Elle aide au diagnostic ; elle ne déclenche rien. Niveau 1.

Le point de rupture. Le déploiement sur plusieurs usines, connecté aux logiciels de pilotage de la production, de gestion et de planification, fait entrer l'IA dans le flux « de l'écart qualité à la décision de production ». Or les références matière, les unités, les seuils de tolérance et les règles de mise en quarantaine varient selon le site, le produit ou le client. Un commentaire d'opérateur est une hypothèse, pas une mesure. Une recommandation erronée de blocage ou d'ajustement peut toucher la qualité, la sécurité ou les livraisons.

La leçon. On distingue trois gestes : détecter, recommander, agir. Chacun exige des données qualifiées, des règles explicites, une personne habilitée et une traçabilité adaptée. Sans langage commun sur les objets métier, relier les systèmes ne lève pas l'ambiguïté [5]. Ouvrir automatiquement un ticket d'analyse sur un écart précisément défini peut relever du niveau 3 ; toute décision qui touche la production reste au niveau 2.

À retenir. Dans les cinq histoires, l'IA fonctionne. Ce qui casse, c'est une liaison : une définition non partagée, un statut d'information flou, un droit trop large, une frontière de décision franchie sans le dire.

Pour votre comité. *Question à poser :* dans laquelle de ces cinq histoires nous reconnaissons-nous le plus, et sur quel projet en cours ? *Outil :* choisir ce projet comme l'un des trois flux de l'atelier (boîte à outils, outil 5).

Ces histoires ont un point commun : chacune a exigé des investissements qui ne figuraient pas dans le budget du pilote. Comment les lire dans un plan de financement ?

Chapitre 8. Lire un budget d'industrialisation : ce que vous financez vraiment

Quand on présente au comité un budget d'industrialisation de l'IA, il ressemble souvent à une ligne technologique : une plateforme, des connecteurs, des licences. C'est une lecture incomplète. Ce que vous financez, en réalité, c'est **la capacité de l'entreprise à transformer ses flux critiques sans perdre la maîtrise de ses décisions**.

Les sept chantiers du chapitre 5 se traduisent, dans un budget, en six postes d'investissement. Le tableau suivant permet de vérifier qu'aucun n'a été oublié.

Poste d'investissement	Chantiers couverts	Ce qu'il faut voir dans le budget
La vérité opérationnelle	1	Du temps d'experts métier pour décrire le flux réel, exceptions comprises
Les données et les connexions	2, 3	Référentiels, qualité, règles de partage, surveillance des connexions
La sécurité et le contrôle	3	Droits bornés, journaux, mécanisme de suspension
Le modèle opérationnel	4, 7	Des rôles nommés et du temps alloué pour les tenir
La preuve	5	Indicateurs mesurés avant le lancement, seuils de décision
L'apprentissage	6, 7	Formation liée aux flux, revues régulières du portefeuille

La vérité opérationnelle. Décrire le flux tel qu'il se déroule vraiment, avec ses contournements, ses exceptions et ses arbitrages, prend du temps à des personnes qui en manquent. C'est moins spectaculaire qu'une démonstration. C'est pourtant ce qui évite de brancher l'IA sur une procédure théorique que plus personne ne suit.

Les données et les connexions. Toutes les données n'ont pas besoin d'être parfaites pour un premier usage. En revanche, toute donnée qui déclenche une action importante doit avoir un statut, un propriétaire et un niveau de confiance connu. Dans l'histoire du prologue, c'est ce poste qui aurait évité la confusion sur les « clients actifs » et la connexion cassée.

La sécurité et le contrôle. L'agence européenne de cybersécurité, l'ENISA, recommande une approche en couches : d'abord les fondamentaux de la cybersécurité, puis les mesures propres à l'IA, puis les exigences sectorielles [24]. Autrement dit, une IA sophistiquée ne compense jamais un socle de sécurité fragile.

Le modèle opérationnel. Une équipe centrale peut fournir des standards, des briques réutilisables, une méthode d'évaluation et une expertise juridique et sécurité. Les métiers gardent la propriété du résultat et de la transformation de leur flux. La bonne organisation n'est ni tout centralisée ni tout décentralisée : c'est celle qui rend visibles les responsabilités de bout en bout et tranche vite.

La preuve. Définir avant le lancement les indicateurs de qualité, de délai, de reprise, de risque et de valeur, ainsi que les seuils qui conduiront à élargir, corriger, suspendre ou arrêter. Cette discipline protège contre deux tentations : poursuivre un outil parce qu'il impressionne, ou abandonner trop tôt une transformation qui demandait quelques ajustements. Les économistes parlent d'une « courbe en J » : la productivité mesurée peut d'abord stagner, voire reculer, pendant que l'entreprise investit dans des actifs invisibles (processus, données, compétences), avant que les bénéfices n'apparaissent [4]. Ce n'est pas une promesse de gains futurs ; c'est un rappel qu'il faut juger un programme sur des indicateurs posés à l'avance, et non sur l'impression des premiers mois.

L'apprentissage. Une entreprise mature ne cherche pas à rendre tous ses flux autonomes. Elle apprend, flux par flux, quel degré d'assistance est pertinent, où la qualité des données limite l'automatisation, où le contrôle humain apporte encore de la valeur et où une intégration plus poussée devient justifiée. C'est ce qui transforme une succession de paris isolés en un portefeuille de décisions assumées.

À retenir. Un budget d'IA qui ne finance que l'outil finance en réalité un pilote de plus. Les liaisons coûtent du temps, de l'organisation et de la discipline, et ce sont elles qui rendent l'outil rentable.

Pour votre comité. *Question à poser :* dans ce budget, quelle part finance l'outil, et quelle part finance les liaisons qui le rendront fiable ? *Outil :* le tableau des six postes ci-dessus, et les trois familles d'indicateurs (boîte à outils, outil 4).

Retour au comité du prologue, en octobre.

Épilogue : revenir à la question de départ

En octobre, le comité du prologue se demandait si son projet « marchait, oui ou non ». Ce guide propose de remplacer cette question binaire par une question plus utile : **quels flux voulons-nous rendre plus capables grâce à l'IA, et quelles liaisons devons-nous renforcer pour que cette capacité reste digne de confiance à l'échelle ?**

Posée ainsi, la réponse n'est plus un verdict sur un outil. C'est un plan : des flux choisis, des liaisons identifiées, des niveaux d'autonomie assumés action par action, des indicateurs posés à l'avance. Un plan que le comité peut suivre, ajuster et défendre.

Boîte à outils

Sept outils, à utiliser dans l'ordre ou séparément. Ils ne remplacent pas une analyse détaillée de processus, de sécurité ou de conformité ; ils servent à faire émerger, en peu de temps, les liaisons qui décideront du passage à l'échelle.

Outil 1. Les dix questions avant de valider un passage à l'échelle

À cocher en séance. Une case qui reste vide n'est pas un refus : c'est un chantier à financer.

- ☐ Savons-nous ce que le pilote a prouvé, et ce qu'il n'a pas encore prouvé ? (*chapitre 1*)
- ☐ Le flux complet est-il décrit tel qu'il se déroule vraiment, contournements compris ? (*chapitre 2*)
- ☐ Pour chaque donnée critique, connaissons-nous la source qui fait foi, son propriétaire et sa fraîcheur ? (*chapitre 2*)
- ☐ L'IA agit-elle avec les droits de l'utilisateur, et ce sont bien nos logiciels qui vérifient les autorisations ? (*chapitres 3 et 5*)
- ☐ Pour chaque geste de l'IA, à quel niveau sommes-nous (suggérer, préparer, exécuter, orchestrer), et qui l'a décidé ? (*chapitre 4*)
- ☐ Les validations humaines prévues sont-elles réelles, et placées avant toute action irréversible ? (*chapitre 4*)
- ☐ Un propriétaire de bout en bout est-il nommé, avec le droit d'arrêter le système ? (*chapitre 5*)
- ☐ Les indicateurs de qualité, de flux et de conséquences ont-ils été mesurés avant le lancement ? (*chapitres 5 et 8*)
- ☐ Savons-nous mettre en pause, revenir en arrière et reconstituer ce qui s'est passé ? (*chapitre 4*)
- ☐ Notre rôle au sens du règlement sur l'IA et l'analyse RGPD sont-ils établis pour cet usage précis ? (*chapitre 6*)

Outil 2. La carte des trois flux

Choisissez trois flux aux conséquences différentes : un qui crée ou protège du chiffre d'affaires, un qui délivre une opération ou un service, un qui attribue ou contrôle un droit important (une dépense, un accès, un engagement contractuel, une décision concernant une personne). Réunissez le responsable métier, le responsable du processus, **une personne qui fait le travail au quotidien**, le représentant des

données ou du logiciel concerné, et la sécurité, le délégué à la protection des données ou la conformité si le flux le justifie.

Règle d'or : quand personne ne connaît la réponse, écrivez « inconnu ». C'est déjà une information précieuse.

À cartographier	Flux 1	Flux 2	Flux 3
Nom du flux et résultat métier attendu			
Ce qui le déclenche, ce qui le termine vraiment			
Les étapes réelles, contournements compris			
Les décisions et les exceptions			
Données critiques : source, propriétaire, fraîcheur			
Logiciels, fichiers et prestataires reliés			
Qui a le droit de faire quoi, jusqu'à quel montant			
Gestes confiés à l'IA et niveau de chacun : suggérer, préparer, exécuter, orchestrer			
Validation humaine et droit d'arrêt			
Jusqu'où une erreur ou un abus pourrait se propager			
Traces, preuves et indicateurs de valeur et de risque			
Décision : garder le niveau actuel, monter d'un niveau, ou d'abord régler une dépendance			

Après l'atelier, ne cherchez pas une note globale. Cherchez les liaisons non résolues. Un flux prometteur peut exiger d'abord un chantier de référentiel ou de droits. À l'inverse, un flux qui paraît simple doit rester aux niveaux 1 ou 2 tant que l'entreprise ne sait pas comprendre, surveiller et contenir les actions associées.

Outil 3. Le permis d'autonomie

Un permis par action, et non par outil. Il est porté par le propriétaire métier et accordé par le comité. Il fixe noir sur blanc ce que l'IA peut faire seule, ce qu'elle doit faire valider et ce qu'elle ne fera jamais, ainsi que les conditions dans lesquelles ce droit peut évoluer ou être retiré. La méthode complète, avec un exemple rempli, figure dans le livre blanc *Le curseur d'autonomie*.

Rubrique	Question à renseigner	Votre réponse
Usage et finalité	Quel problème est résolu, quelle valeur est attendue, comment la mesure-t-on ?	
Action concernée	Que l'IA peut-elle lire, préparer, créer, modifier, envoyer ou coordonner ?	
Niveau autorisé	Niveau 1 à 4, date d'effet, date de revue	
Périmètre	Données, outils, droits, montants, volumes, horaires, zones, exclusions	
Interdits	Ce que l'IA ne fera jamais, même pour atteindre l'objectif	
Décision et supervision	Porteur, valideur, destinataire des alertes, qui peut arrêter et redémarrer	
Preuves	Tests, sources de référence, indicateurs, incidents connus, journalisation	
Résilience	Dépendances critiques, mode dégradé, procédure de repli, date du dernier exercice	
Révision	Événements qui déclenchent une réévaluation ; conditions de progression et de recul	

Outil 4. Les trois familles d'indicateurs de valeur

Famille	Ce qu'elle mesure	Exemples
Qualité du résultat	Ce que l'IA produit	Taux d'exactitude vérifié sur échantillon, sources traçables, complétude
Qualité du flux	Ce que devient le travail autour	Délai de bout en bout, taux de reprise, escalades, actions annulées, charge déplacée vers le contrôle
Conséquences	Ce que vit l'entreprise	Réclamations, incidents, écarts financiers, signalements, satisfaction des clients et des collaborateurs

Mesurez ces trois familles **avant** le lancement, pour disposer d'un point de départ. Sans référence, aucun gain ne peut être démontré, et aucune dérive ne peut être repérée. C'est précisément ce qui manquait au comité du prologue en octobre.

Outil 5. L'atelier de comité (2 h)

Objectif : sortir de la séance avec une première cartographie de trois flux et trois chantiers prioritaires.

Participants : direction générale, DAF, DSI, les propriétaires métier des flux choisis, et selon le cas juridique, conformité ou protection des données.

1. **Cadrage (15 min).** Le dirigeant sponsor explique pourquoi l'entreprise regarde l'IA par les flux, et le groupe choisit les trois flux à étudier.
2. **Récit du flux réel (30 min).** La personne qui fait le travail raconte un cas récent, du déclencheur au résultat. Les autres écoutent sans corriger.
3. **Repérage des liaisons (30 min).** On remplit la carte des trois flux (outil 2), en notant « inconnu » sans hésiter.
4. **Simulation de cascade (20 min).** Pour chaque flux, on se demande : « si l'IA se trompe ici, jusqu'où l'erreur va-t-elle ? »
5. **Niveaux d'autonomie (15 min).** On fixe, geste par geste, le niveau raisonnable aujourd'hui et la preuve nécessaire pour monter d'un cran.
6. **Décisions (10 min).** Trois chantiers prioritaires, un responsable pour chacun, une date de revue.

Outil 6. Cinq signaux qu'un projet n'est pas prêt

- Personne ne peut dire qui a le droit d'arrêter le système.
- L'assistant utilise un compte technique aux droits plus larges que ceux de ses utilisateurs.
- Le succès est mesuré uniquement par la satisfaction des premiers utilisateurs.
- Les exceptions sont « gérées par l'équipe projet », sans être décrites nulle part.
- On ne sait pas reconstituer ce que l'IA a lu, produit et déclenché la semaine dernière.

Outil 7. Glossaire pour le comité

Terme	En clair
Agent (IA agentique)	Système d'IA qui peut utiliser des outils et enchaîner des actions dans des logiciels, pas seulement produire du texte
API	« Prise » logicielle qui permet à un programme de lire une information dans un autre ou de lui demander d'agir
Confabulation	Production assurée d'une information fausse par une IA ; on parle aussi d'hallucination
CRM, ERP, GMAO, MES	Logiciels de gestion : relation client, gestion intégrée de l'entreprise, maintenance, pilotage de la production
Dépoyeur	Au sens du règlement sur l'IA, l'organisation qui utilise un système d'IA dans son activité professionnelle
Flux	Enchaînement réel d'étapes, de décisions et de transmissions qui transforme un déclencheur en résultat métier
Fournisseur	Au sens du règlement sur l'IA, celui qui développe un système d'IA et le met sur le marché ou en service sous son nom
Injection d'instructions	Texte malveillant, souvent caché dans un document ou un courriel, qui cherche à détourner le comportement d'une IA
Journalisation	Enregistrement de ce que fait le système, quand, avec quelles données et quelle version
Liaison	Ce qui permet à une étape du flux de recevoir l'information, le droit ou la décision dont la suivante a besoin
Moindre privilège	Principe consistant à ne donner à un système que les accès strictement nécessaires à sa tâche
Modèle	« Moteur » d'IA qui comprend et génère du texte ; il ne constitue qu'une partie du système
Niveaux d'autonomie	Suggérer, préparer, exécuter, orchestrer : les quatre réglages possibles d'un geste confié à l'IA (méthode U-CIE)

Terme	En clair
Permis d'autonomie	Autorisation écrite, datée et révocable qui fixe ce qu'une IA peut faire seule pour une action donnée (méthode U-CIE)
Pilote	Expérimentation sur un périmètre restreint et protégé, destinée à vérifier l'utilité d'un usage
Prompt	Consigne ou question adressée à l'IA
Référentiel	Source de données reconnue comme faisant foi pour un objet métier (un client, un équipement, un contrat)
Sémantique	Sens donné aux mots et aux données ; deux logiciels peuvent être connectés sans partager le même sens
Système à haut risque	Catégorie du règlement européen sur l'IA (emploi, crédit, éducation, etc.) soumise à des obligations renforcées à partir du 2 décembre 2027

À propos de U-CIE

U-CIE aide les entreprises à penser, construire et piloter leur IA de A à Z. Plutôt que d'ajouter un outil de plus, nous commençons par cartographier avec vos équipes la façon dont votre entreprise fonctionne vraiment, pour repérer où l'IA peut changer la donne.

Penser. Cartographier les flux qui comptent et les liaisons à consolider avant tout passage à l'échelle.

Construire. Concevoir avec vous des usages d'IA générative ou agentique, en fixant pour chacun ce qu'il peut faire seul, ce qu'il doit faire valider et ce qu'il ne fera jamais.

Piloter. Installer les indicateurs, les revues et les règles qui permettent de mesurer la valeur, de surveiller les risques et de faire évoluer l'autonomie au rythme de ce que l'entreprise sait maîtriser.

Notre conviction tient en une phrase : l'IA doit transformer votre entreprise sans jamais vous échapper.

Pour cartographier vos trois premiers flux critiques avec votre comité de direction, contactez U-CIE sur u-cie.com.

Références

État du droit et des sources vérifié au 25 octobre 2026.

1. OCDE, [The Adoption of Artificial Intelligence in Firms: New evidence for policy making](#)
2. NIST, [Artificial Intelligence Risk Management Framework \(AI RMF 1.0\)](#)
3. NIST, [AI RMF Playbook: Map](#)
4. Brynjolfsson, Rock, Syverson, [The Productivity J-Curve: How Intangibles Complement General Purpose Technologies](#), NBER
5. Centre commun de recherche (JRC), [Artificial Intelligence for Interoperability in the European Public Sector](#)
6. OWASP, [Top 10 for LLM Applications v2025](#)
7. NSA, CISA et partenaires, [Deploying AI Systems Securely](#)
8. NIST, [AI RMF Playbook: Measure](#)
9. NIST, [Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations](#)
10. NIST, [AI RMF: Generative Artificial Intelligence Profile](#)
11. Union européenne, [Règlement sur l'intelligence artificielle, texte consolidé](#)
12. NCSC, [Thinking carefully before adopting agentic AI](#)
13. Gouvernement britannique, [Guidelines and best practices for making government datasets ready for AI](#)
14. Commission européenne, [Ethics guidelines for trustworthy AI](#)
15. DSIT, [Portfolio of AI assurance techniques](#)
16. ISO, [ISO/IEC 42001:2023, Artificial intelligence: Management system](#)
17. OCDE, [Skill needs and policies in the age of artificial intelligence](#)
18. OCDE, [Using AI in the workplace: Opportunities, risks and policy responses](#)
19. NCSC, [Thinking about the security of AI systems](#)
20. Union européenne, [Règlement général sur la protection des données](#)
21. Comité européen de la protection des données, [Avis 28/2024 sur les modèles d'IA](#)
22. Union européenne, [Règlement \(UE\) 2026/1744, omnibus numérique sur l'IA](#)
23. CNIL, [Comment déployer une IA générative ? La CNIL apporte de premières précisions](#)
24. ENISA, [Multilayer Framework for Good Cybersecurity Practices for AI](#)
25. Commission européenne, [L'Omnibus de l'IA entre en vigueur](#), 27 juillet 2026
26. AI Act Explorer, [Digital Omnibus : remplacement de l'article 4](#)