

# L'IA au service de l'Audit Interne

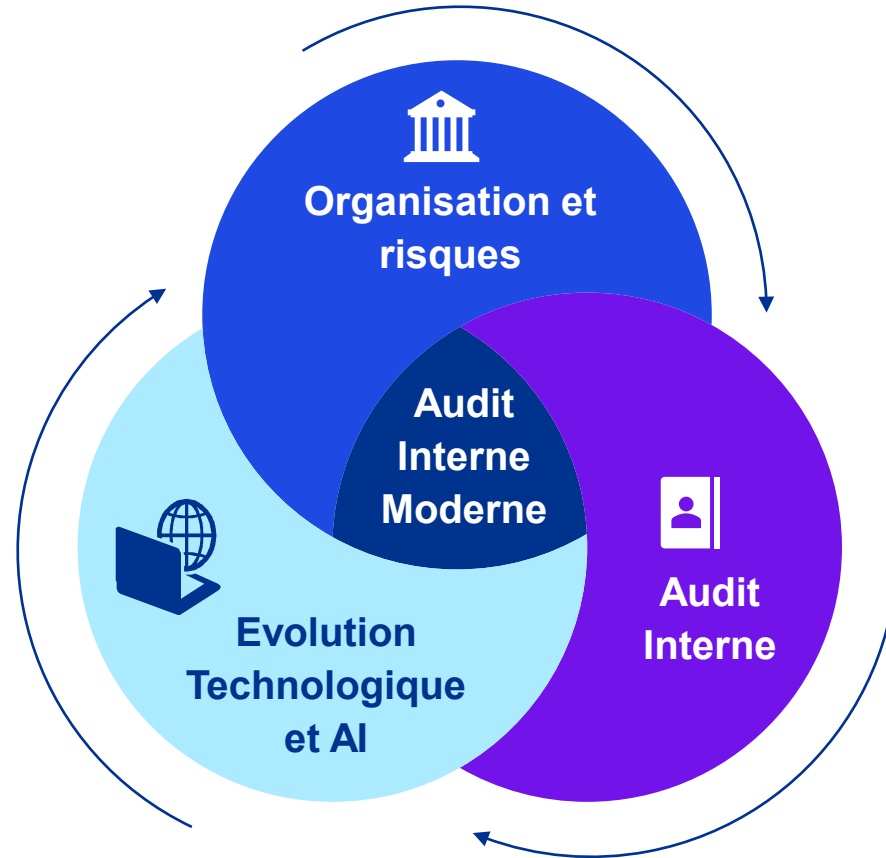
Raphaël Schair – Julien Stocq

15/01/2026





# L'IA et l'audit interne ... comprendre le nouveau terrain de jeu





## Nos Objectifs Aujourd'hui...

Démystifier l'IA pour l'auditeur interne

Montrer comment l'IA peut renforcer la chaîne de valeur de l'Audit Interne

Identifier les conditions d'un usage maîtrisé et crédible de l'IA

Positionner clairement le rôle de l'audit interne



## Agenda

- 01 IA... de quoi parle-t-on vraiment ?
- 02 L'IA et l'Audit Interne: où se crée la valeur?
- 03 Les risques à suivre pour l'Audit Interne
- 04 Le rôle de l'Audit Interne
- 05 Et maintenant? Cap vers 2030



**Raphaël Schair**  
Director - KPMG Advisory  
Enterprise Risk &  
Assurance

T: +32 498 21 07 04  
[rschair@kpmg.com](mailto:rschair@kpmg.com)



**Julien Stocq**  
Transformation Digitale  
Partner - KPMG Wallonie  
T: +32 476 66 16 56

[jistocq@kpmg.com](mailto:jistocq@kpmg.com)

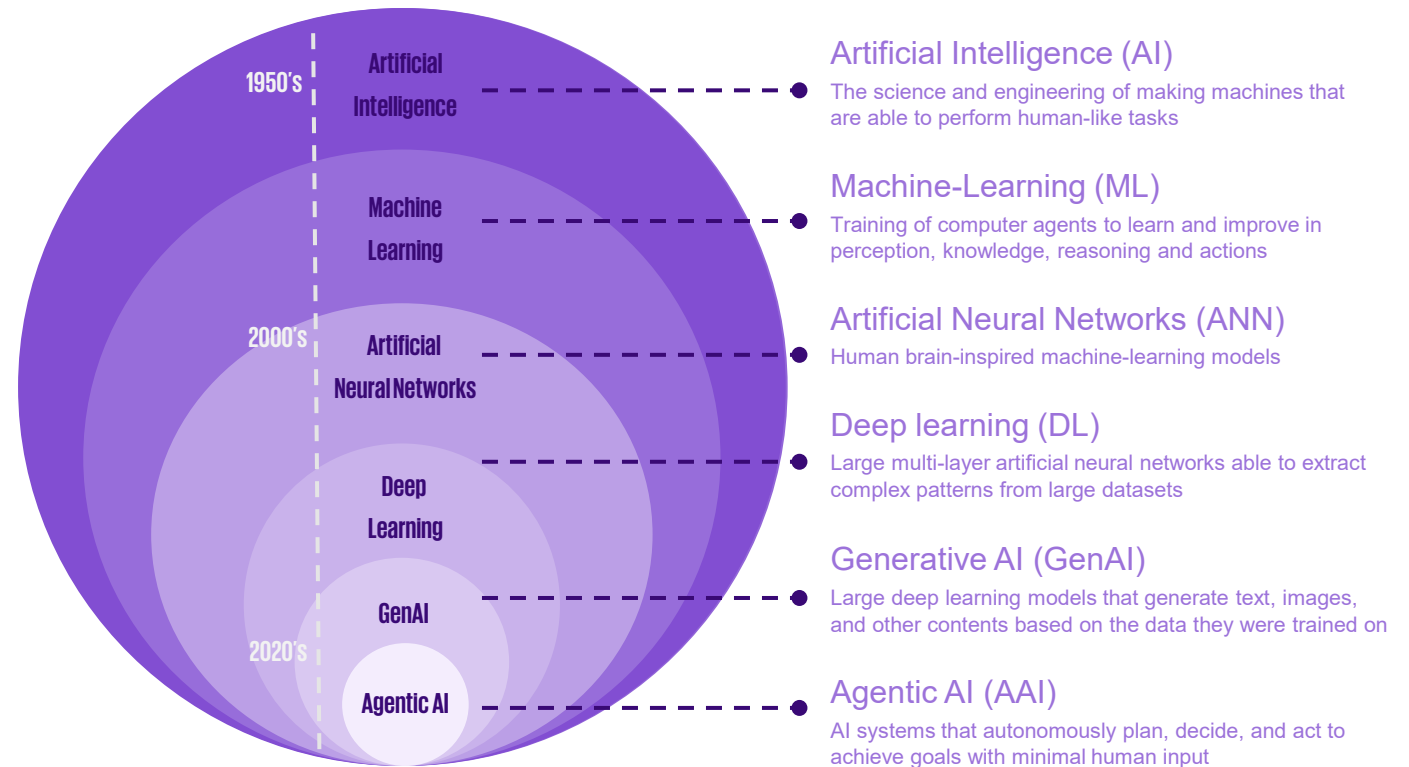


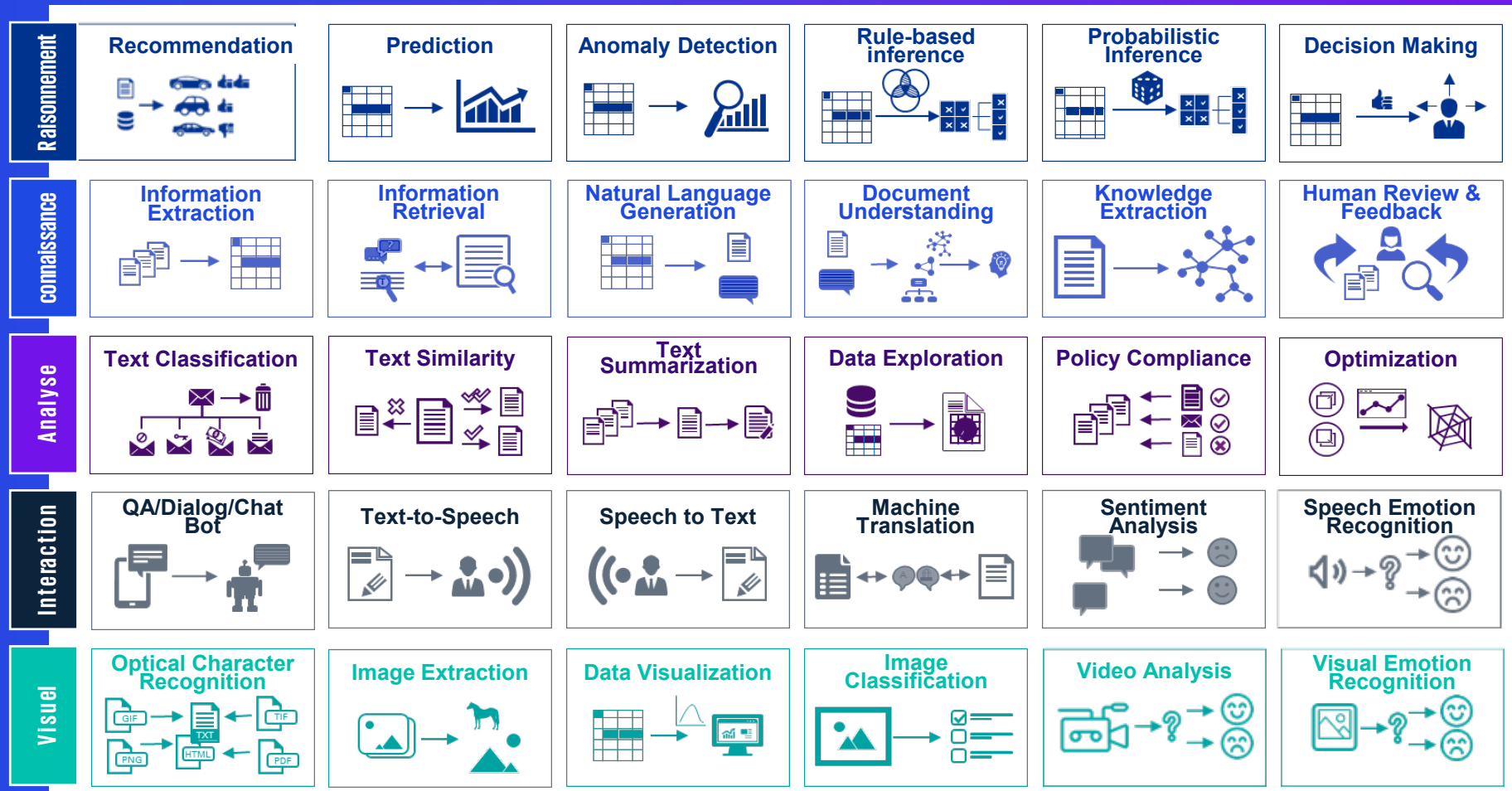
01

# L'IA: de quoi parle-t-on vraiment?

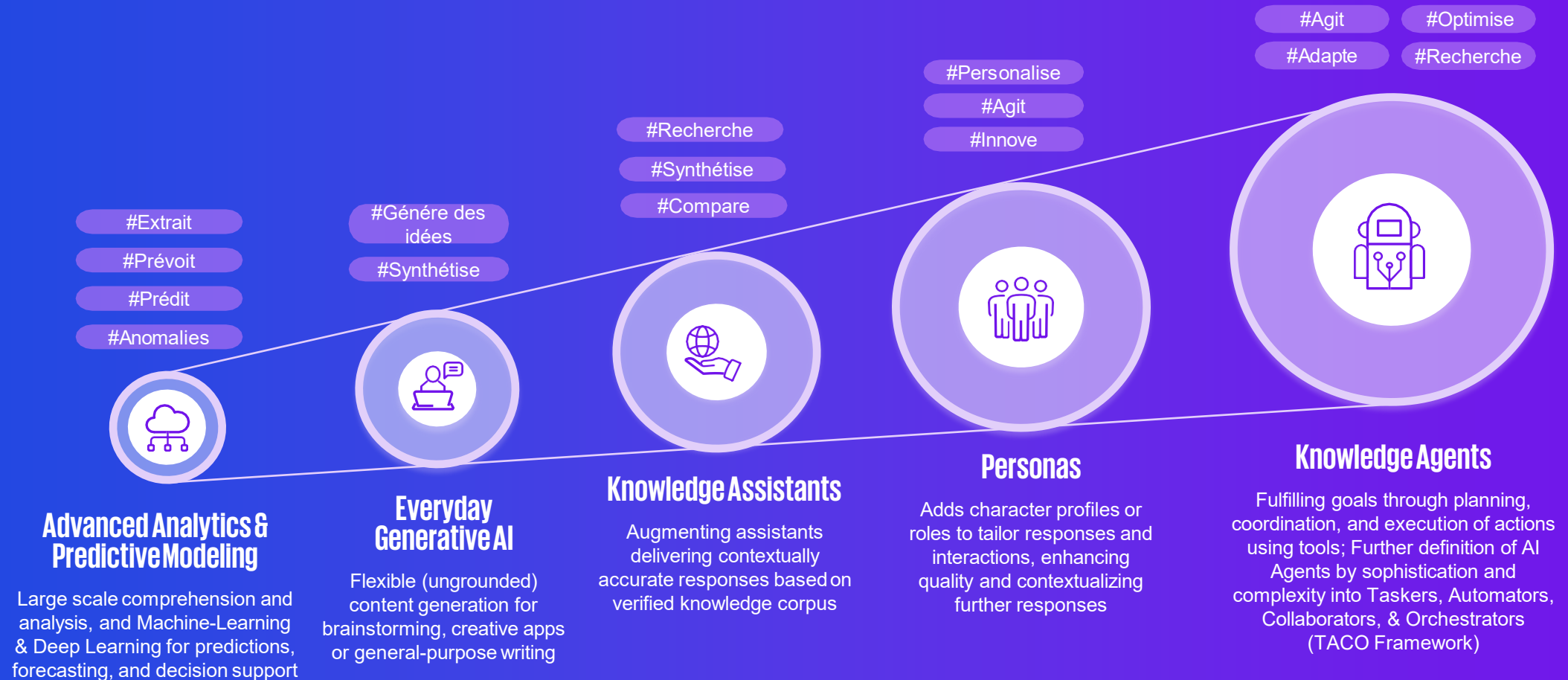


# Evolution de l'IA





# Évolution de l'IA : l'émergence des collaborateurs numériques





# Panorama des outils disponibles pour l'Audit Interne

Un aperçu des grandes catégories d'outils, sans entrer dans la technique

## IA Généralistes

*Très utiles, très accessibles... mais forte vigilance sur les données et la confidentialité*



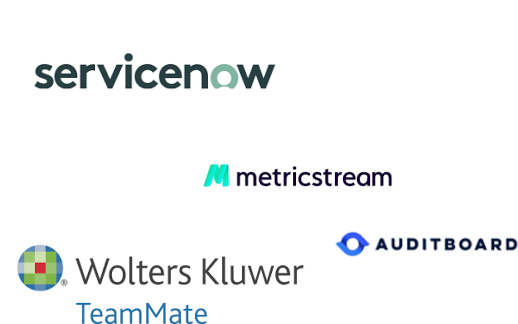
## IA orientées données & analytics

*Très utiles, très accessibles... mais Potentiel élevé, mais attention à la compréhension des modèles et aux faux positifs*



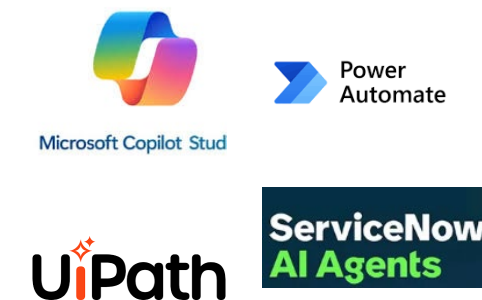
## IA spécialisées Audit/GRC

*Bonne intégration métier, mais dépendance éditeur et paramétrage critique*



## Agents IA (semi-autonomes)

*Agentes métiers -Très prometteur, mais niveau de risque élevé : gouvernance, supervision, responsabilité, traçabilité*



Exemples

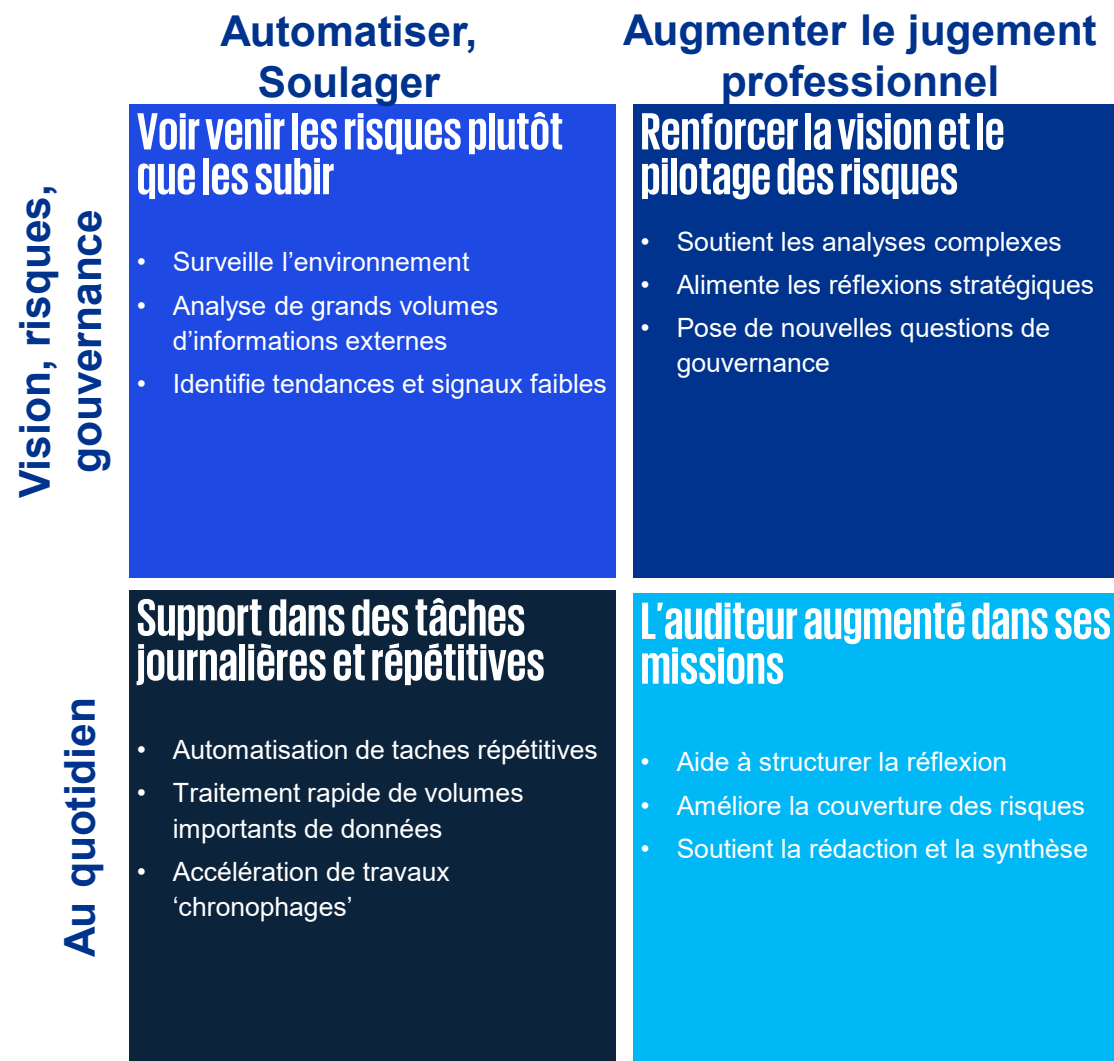


02

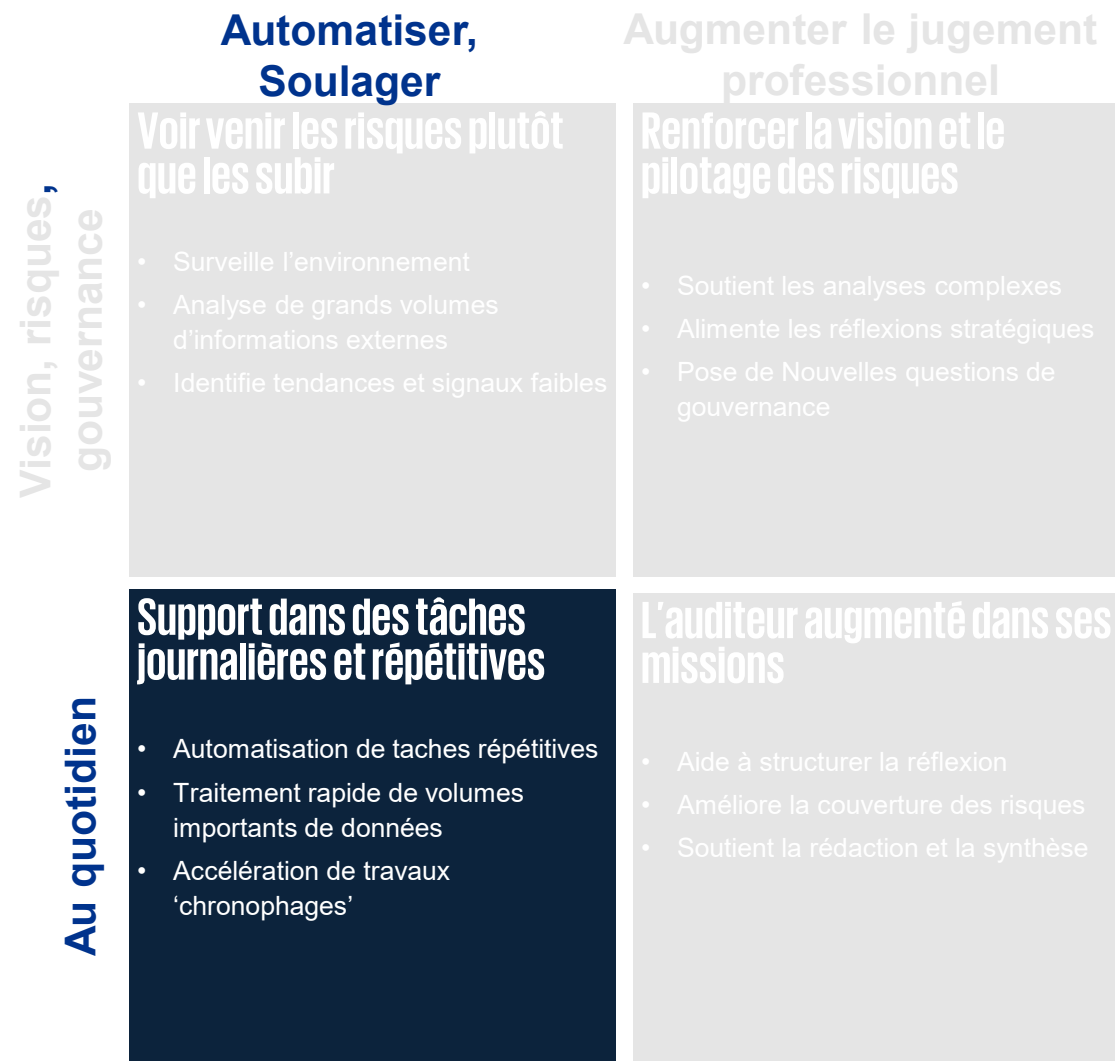
# L'IA et l'Audit Interne: où se crée la valeur?



# L'IA au service de l'Audit Interne

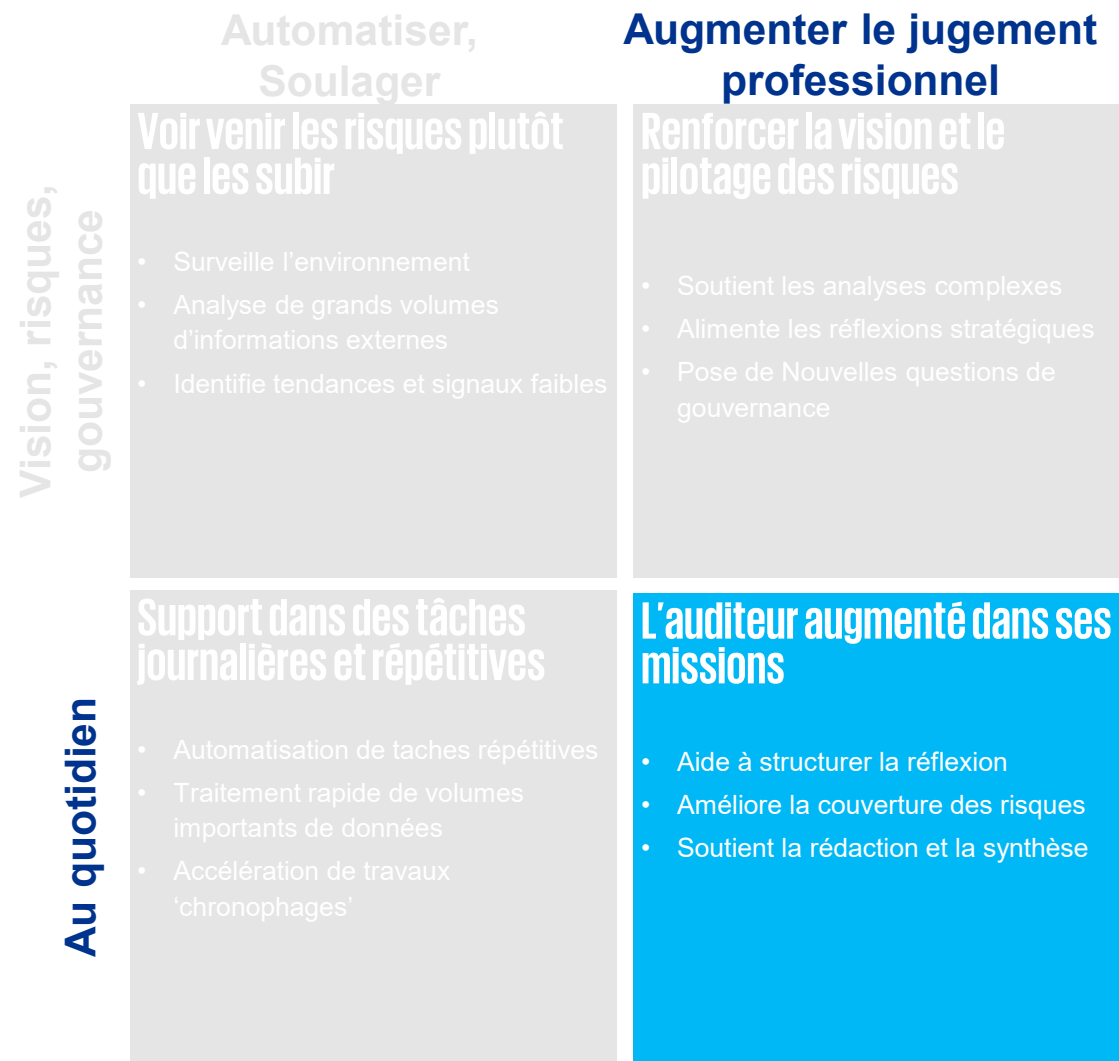


# L'IA au service de l'Audit Interne

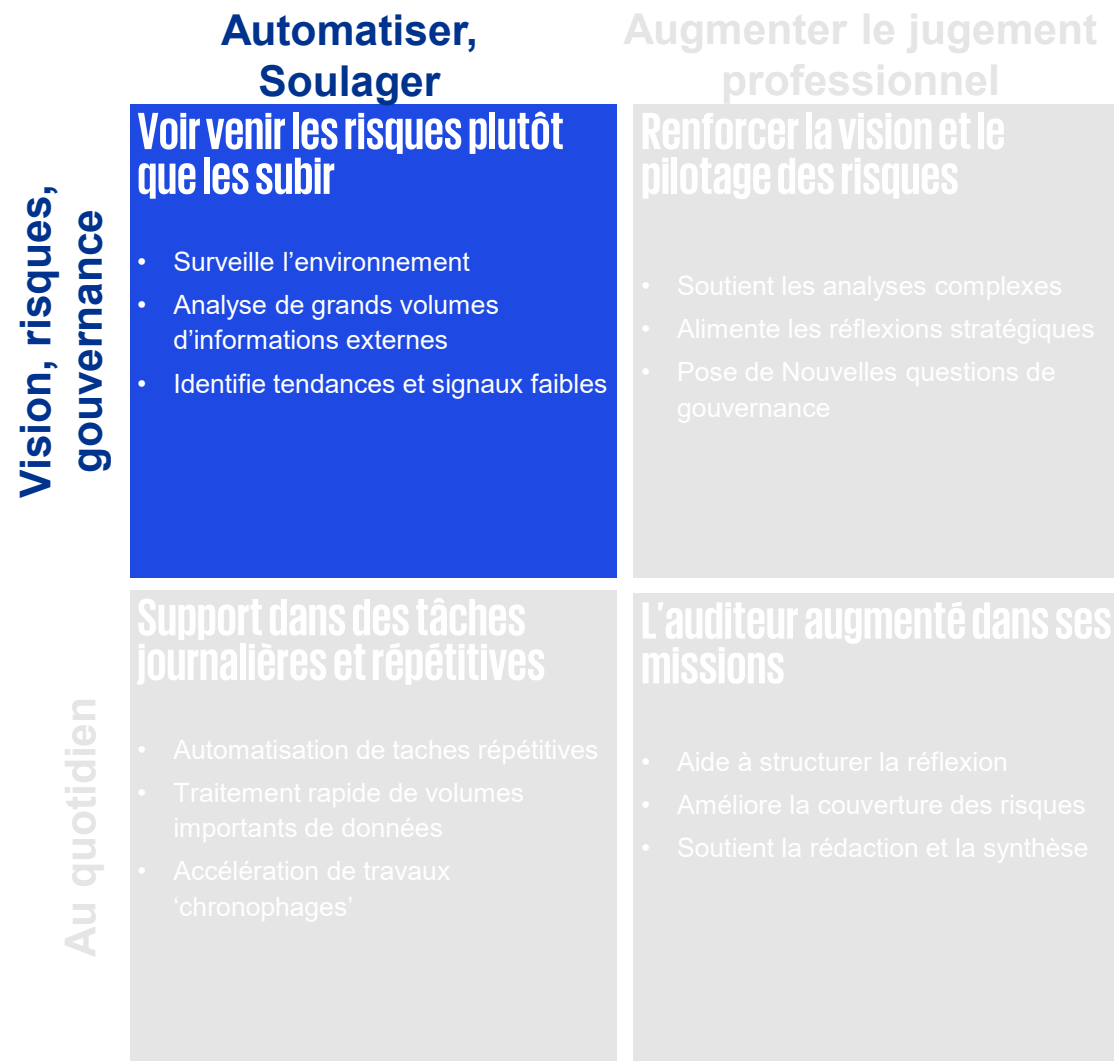




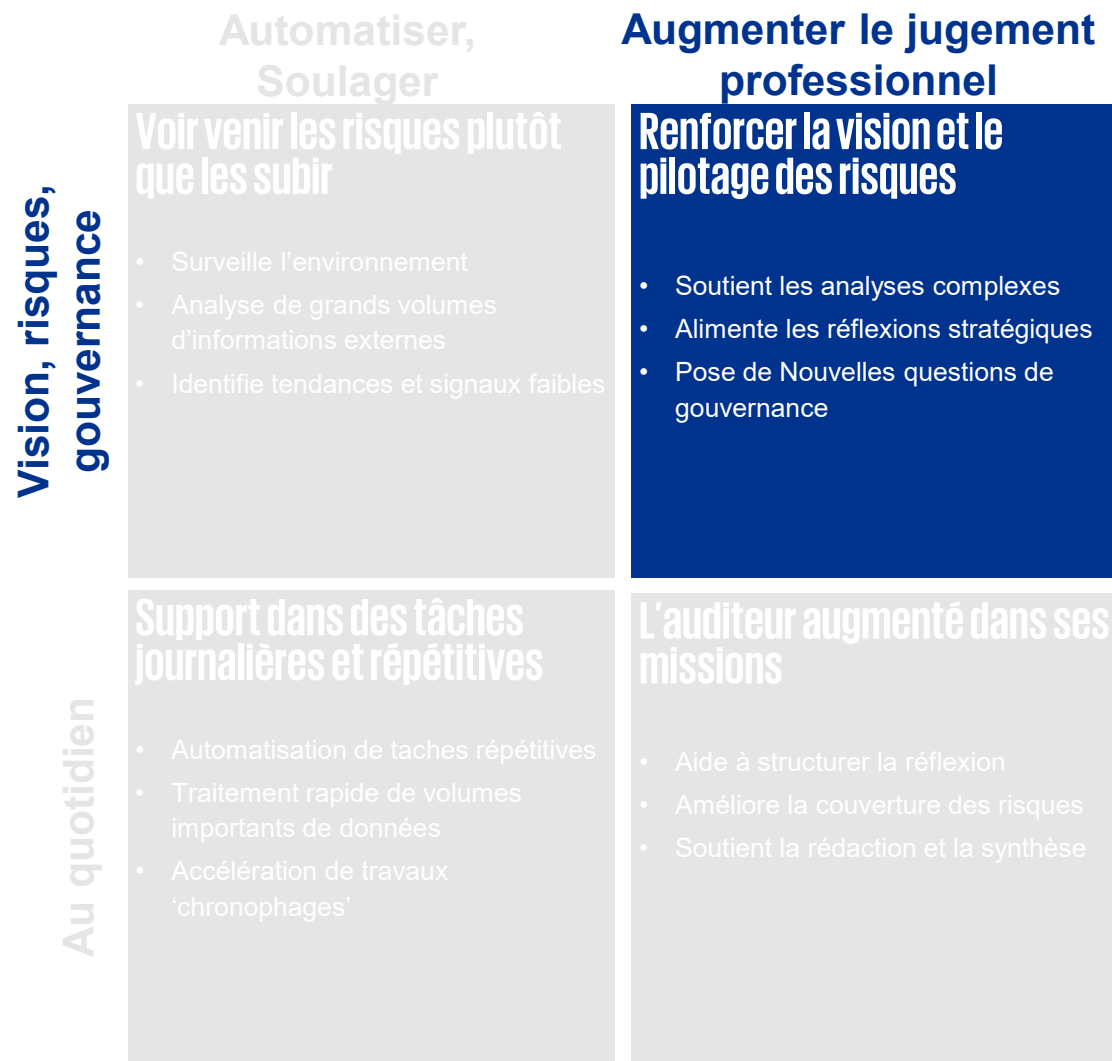
# L'IA au service de l'Audit Interne



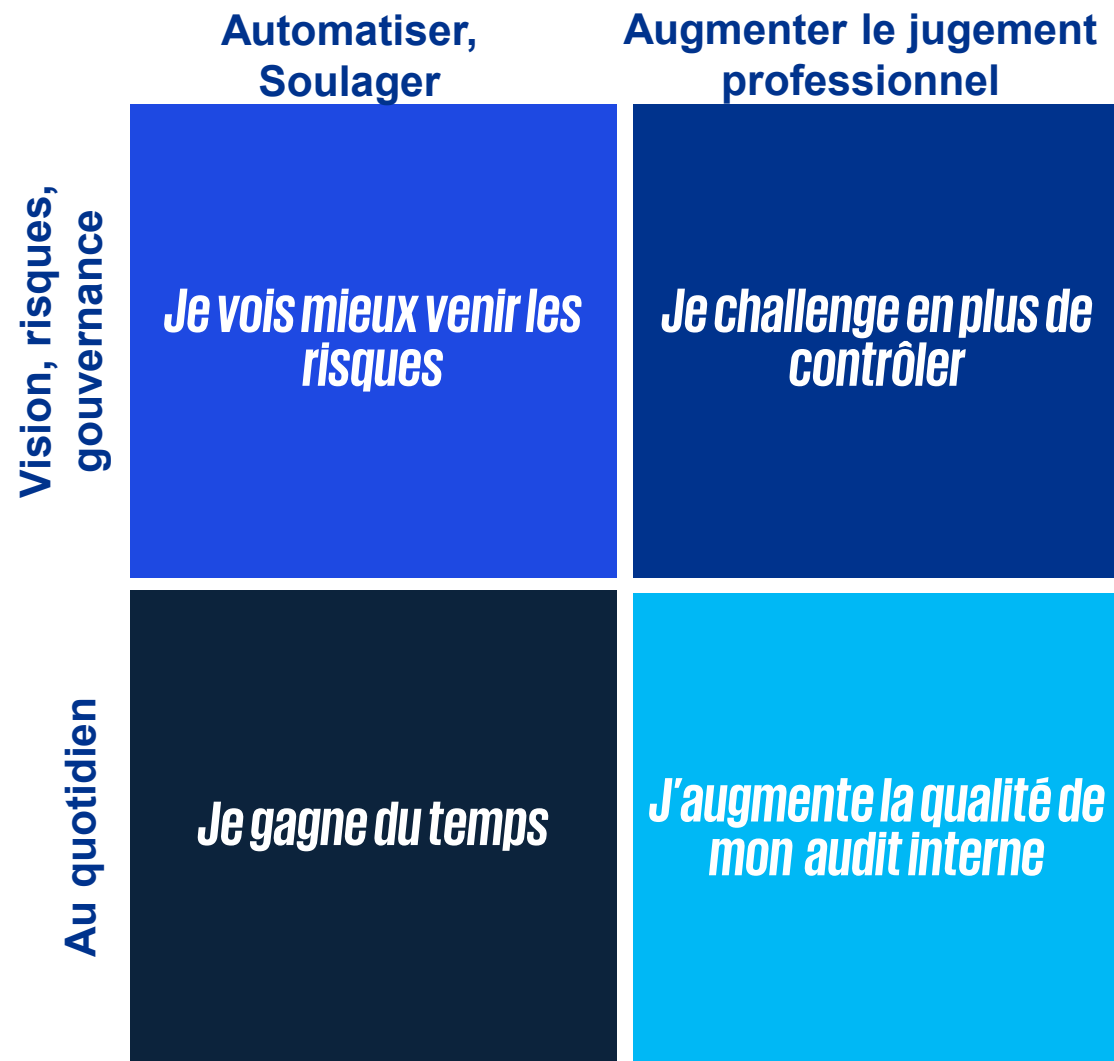
# L'IA au service de l'Audit Interne



# L'IA au service de l'Audit Interne



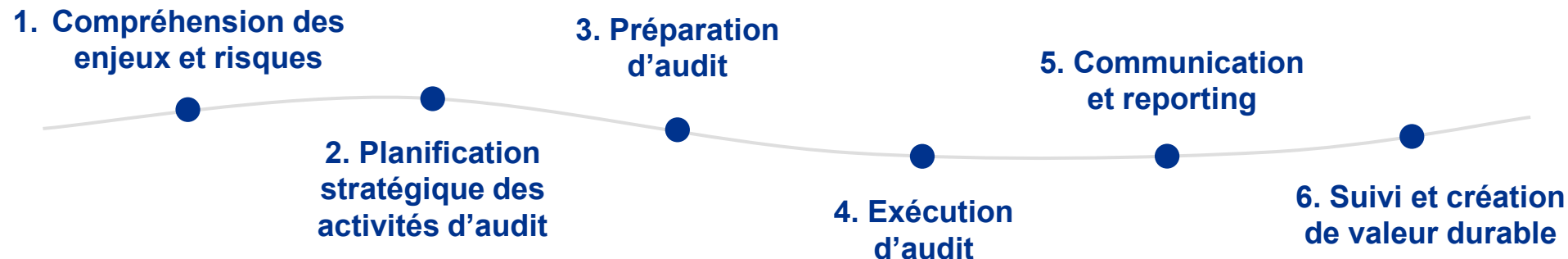
# L'IA au service de l'Audit Interne





# Où se crée la valeur?

De la planification stratégique à l'impact durable sur l'organisation



## 1. Compréhension des enjeux et risques

- Alignement avec la stratégie
- Meilleure pertinence des missions
- Vision orientée risques et priorités business

## 2. Planification stratégique des activités d'audit

- Priorisation des missions à plus forte valeur
- Allocation optimale des ressources
- Vision pluriannuelle cohérente

## 3. Préparation d'audit

- Efficacité de l'exécution
- Clarté du périmètre et des objectifs
- Réduction des zones grises en cours de mission

## 4. Exécution d'audit

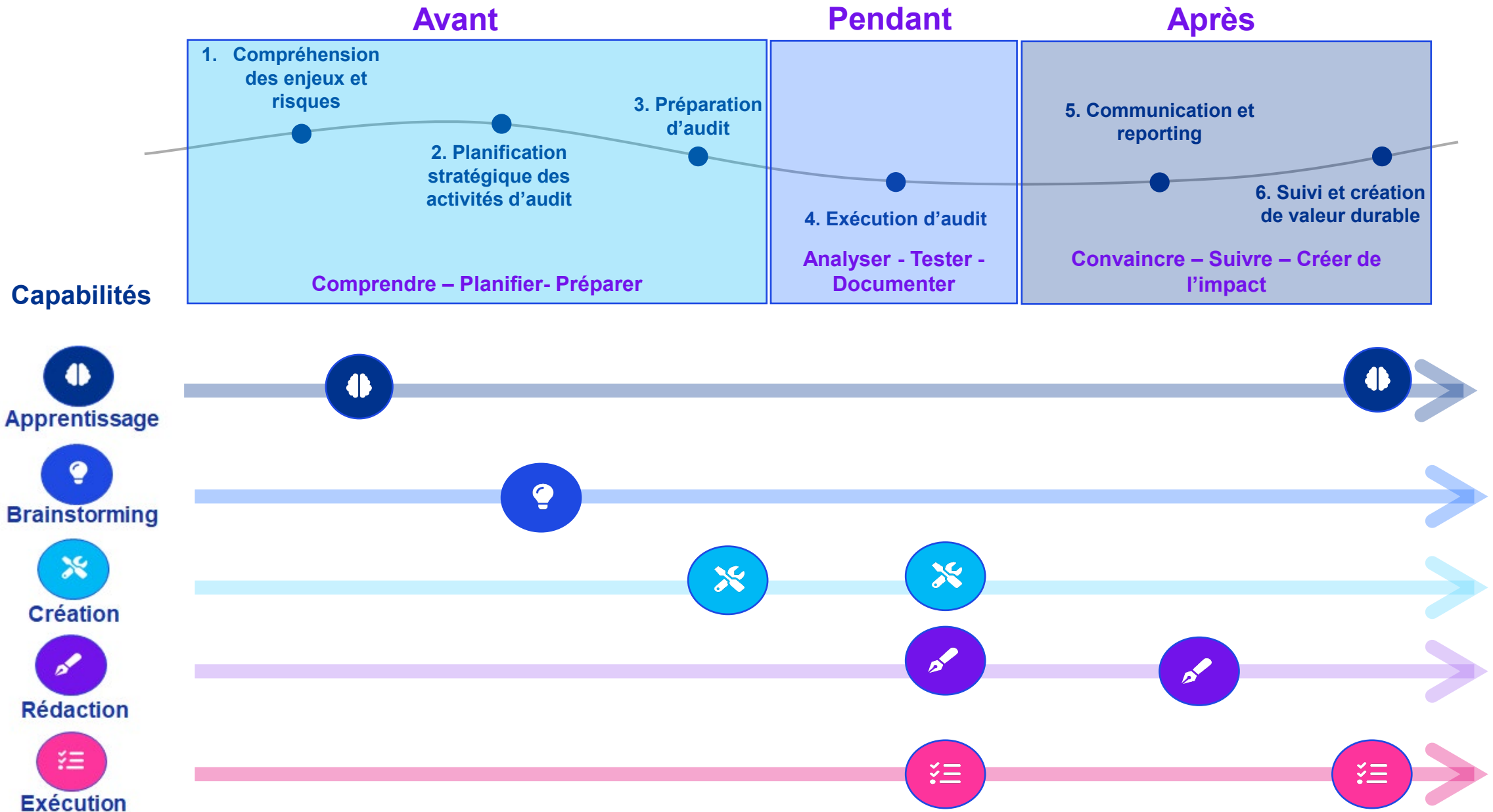
- Assurance indépendante
- Identification des faiblesses de contrôle et identification d'opportunités d'amélioration
- Analyse factuelle et étayée

## 5. Communication et reporting

- Compréhension par le management
- Décisions éclairées
- Crédibilité de la fonction audit

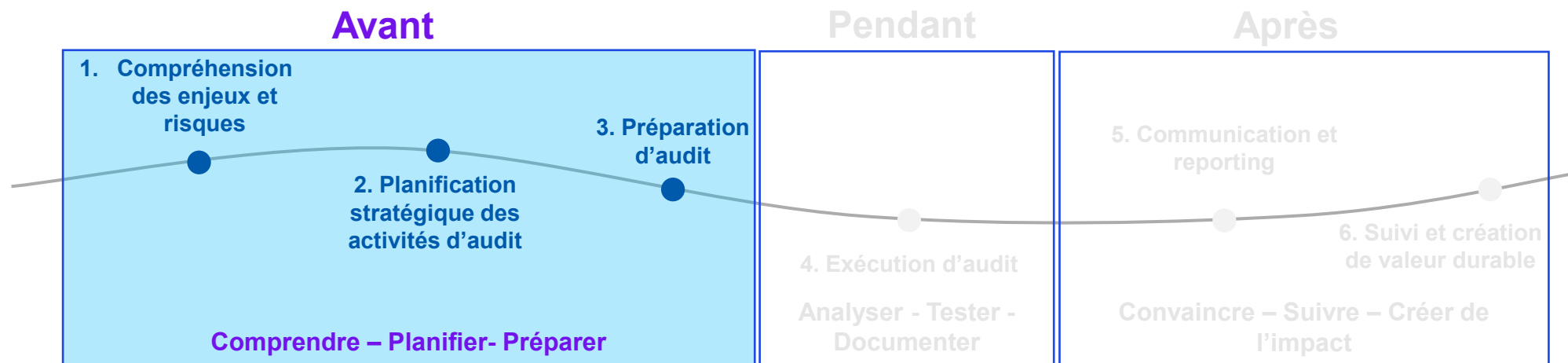
## 6. Suivi et création de valeur durable

- Amélioration réelle des pratiques
- Réduction du risque résiduel
- Contribution continue à la performance



# Avant l'audit : mieux comprendre et mieux préparer

Préparer l'audit, c'est déjà auditer



*Accélérer la montée en connaissance et la préparation*



## Apprentissage

- Comprendre rapidement un processus, un secteur, une réglementation
- Synthétiser/comparer des documents internes et externes
- Analyser rapidement un référentiel ou une norme pour en extraire les points clés pertinents pour l'audit



## Brainstorming

- Identifier et structurer risques, contrôles et angles morts, y compris via des scénarios plausibles (*what could go wrong?*)
- Challenger le plan d'audit
- Challenger le périmètre des audits, en testant des hypothèses alternatives

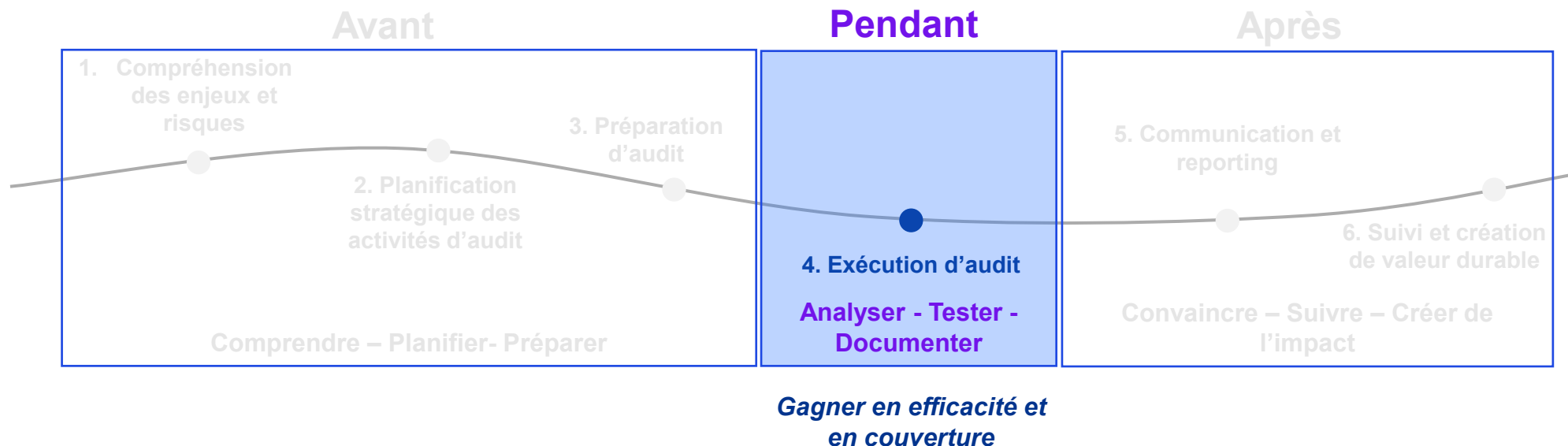


## Création

- Programme d'audit
- Matrice de risques et de contrôles (RCM)
- Questionnaire / Canevas d'entretiens

# Pendant l'audit : analyser et tester plus efficacement

L'IA au service du regard critique de l'auditeur



## Exécution

- Analyser de données sur des populations étendues ou complètes
- Tests automatisés, répétés et contrôlés
- Détecter des anomalies, signaux faibles et schémas atypiques



## Création

- Structurer progressivement des constats d'audit
- Organiser et améliorer la traçabilité des preuves
- Structurer le lien entre constats, risques et impacts



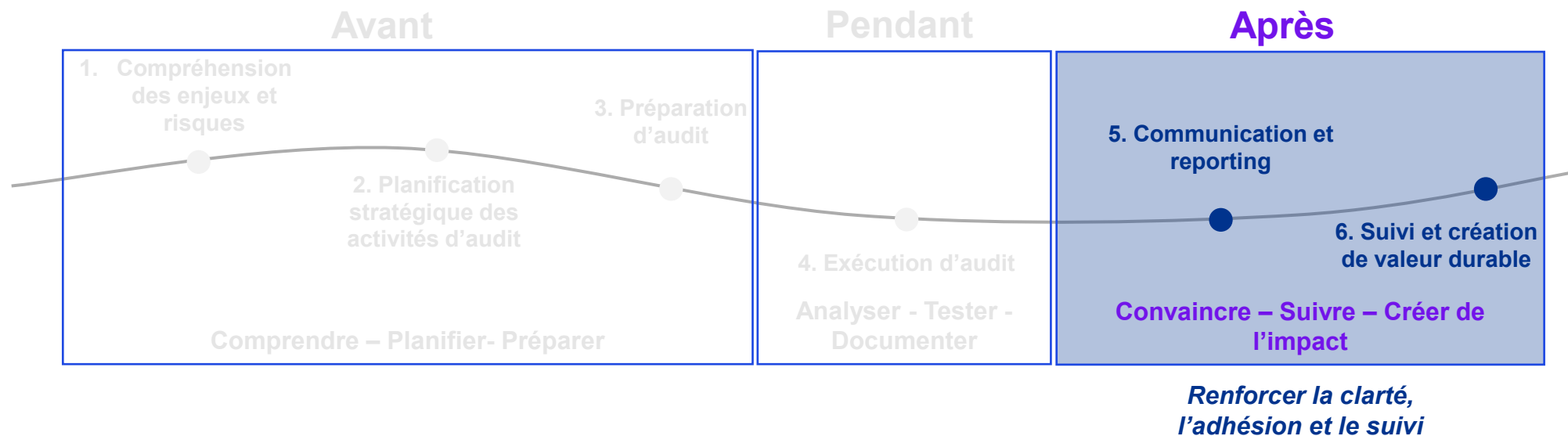
## Rédaction

- Reformuler et clarifier des constats
- Améliorer la structure et la cohérence
- Pré-synthèses intermédiaires pour l'équipe d'audit



# Après l'audit : convaincre et créer de l'impact

Un audit utile est un audit compris et suivi - Passer du constat à l'action



## Rédaction

- Clarifier et prioriser des constats
- Améliorer la structure et la cohérence (=lisibilité) d'un rapport
- Adapter le message au public (management, comité d'audit)



## Exécution

- Suivre des plans d'action
- Consolider et analyser les réponses du management
- Identifier des retards, blocages et tendances récurrentes



## Apprentissage (Analyse et Pilotage)

- Analyser de façon transversale des constats et actions
- Identifier des causes racines récurrentes
- Mettre en évidence des leviers d'amélioration continue



Jobs to Be Done (Top 3)	Identifier les risques clés Analyser l'environnement réglementaire Prioriser les zones à fort impact	Définir le plan annuel d'audit Allouer les ressources efficacement Établir les priorités	Collecter les données pertinentes Définir objectifs & critères Préparer questionnaires	Réaliser les tests Documenter les constats Identifier les écarts	Rédiger le rapport Présenter les résultats Formuler recommandations	Suivre la mise en œuvre Mesurer l'impact Identifier opportunités
Principaux Pains	Volume massif de données Difficulté à anticiper Manque de visibilité	Processus manuel chronophage Mauvaise allocation Difficulté d'alignement	Données dispersées Temps perdu Risque d'oubli	Charge administrative Erreurs humaines Anomalies complexes	Temps de rédaction long Manque de clarté Difficile à personnaliser	Manque de suivi Difficile à mesurer Processus réactif
Comment l'IA peut aider	Analyse prédictive des risques Extraction réglementaire Cartographie dynamique	Optimisation des plans Simulation de scénarios Alignement stratégique	Extraction & structuration automatique Génération de checklists Pré-analyse anomalies	Automatisation des tests Détection anomalies Aide rédaction constats	Génération automatique de rapports Visualisation dynamique Recommandations IA	Tableaux de bord IA Analyse d'impact prédictive Détection proactive
Type de modèle IA	<b>Prédicatif</b> (scoring, forecasting) <b>NLP</b> (analyse réglementaire)	<b>Optimisation</b> <b>Prédicatif</b> (scénarios)	<b>NLP</b> (extraction) <b>Génératif</b> (checklists)	<b>Machine Learning</b> (anomalies) <b>Prédicatif</b> (monitoring)	<b>Génératif</b> (rapports) <b>Visualisation IA</b>	<b>Prédicatif</b> (impact) <b>Prescriptif</b> (recommandations)
Type de données nécessaires (Top 3)	1. Cartographie des risques 2. Données réglementaires 3. Données externes marché	1. Plan d'audit précédent 2. Ressources & budgets 3. Objectifs stratégiques	1. Processus & procédures 2. Données opérationnelles 3. Historique des audits	1. Transactions & logs 2. Données de contrôle interne 3. Échantillons tests	1. Résultats d'audit 2. KPI & indicateurs 3. Feedback parties prenantes	1. Plan d'action 2. KPI post-audit 3. Données de performance
Biais IA	<ul style="list-style-type: none"> <li>Biais dans les données historiques (risques sous-estimés)</li> <li>Surconfiance dans les prédictions</li> <li>Manque de transparence des modèles</li> </ul>	<ul style="list-style-type: none"> <li>Décisions influencées par biais algorithmiques</li> <li>Optimisation non alignée avec objectifs humains</li> <li>Dépendance excessive à l'IA</li> </ul>	<ul style="list-style-type: none"> <li>Mauvaise qualité des données entraînant erreurs</li> <li>Biais linguistiques dans NLP</li> <li>Perte de contexte métier</li> </ul>	<ul style="list-style-type: none"> <li>Mauvaise qualité des données entraînant erreurs</li> <li>Biais linguistiques dans NLP</li> <li>Perte de contexte métier</li> </ul>	<ul style="list-style-type: none"> <li>Mauvaise qualité des données entraînant erreurs</li> <li>Biais linguistiques dans NLP</li> <li>Perte de contexte métier</li> </ul>	<ul style="list-style-type: none"> <li>Mauvaise qualité des données entraînant erreurs</li> <li>Biais linguistiques dans NLP</li> <li>Perte de contexte métier</li> </ul>

# Usages IA en audit interne : maturité et vigilance

Pourquoi tous les usages ne doivent pas être traités de la même manière



*Usages assistés, à faible risque, sous supervision humaine*

- Analyse et synthèse de documents
- Compréhension de processus, de cadres réglementaires
- Aide à la préparation des audits (risques, programmes d'audit, questionnaires)
- Analyses de données et tests automatisés
- Aide à la rédaction de constats et de rapports
- Suivi des plans d'action

***L'IA assiste l'auditeur, sans décider ni conclure à sa place***



*Usages plus sensible, à risque accru*

- Prise de décision automatisée ou semi-automatisée
- Génération de conclusions ou d'opinions d'audit
- Utilisation d'IA sur des données sensibles ou confidentielles
- Déploiement d'outils IA sans gouvernance claire
- Dépendance à des modèles ou fournisseurs externes
- Réduction de la supervision humaine

***Les risques de perte de contrôle, de responsabilité floue et de fausse confiance augmentent fortement.***



03

# Les risques à suivre pour l'Audit Interne





## DEFINE

Business problem

Job to be done

Business impact



## DESIGN

Data & Model type

Model rules & feed

MVP & cycles



## DEPLOY

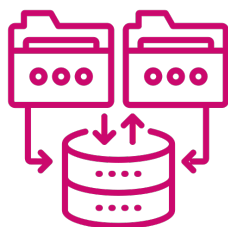
Test & Scale

Change mgt

Gov. & Control



Stratégie &  
Leadership



Data &  
Infrastructure



Cas d'usage



Talents &  
Expertise

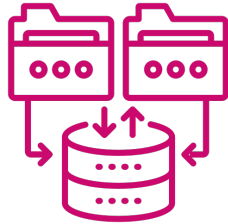


Gouvernance &  
Ethique

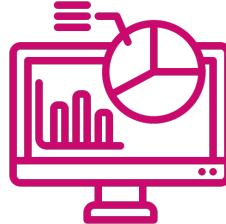




Stratégie &  
Leadership



Data &  
Infrastructure



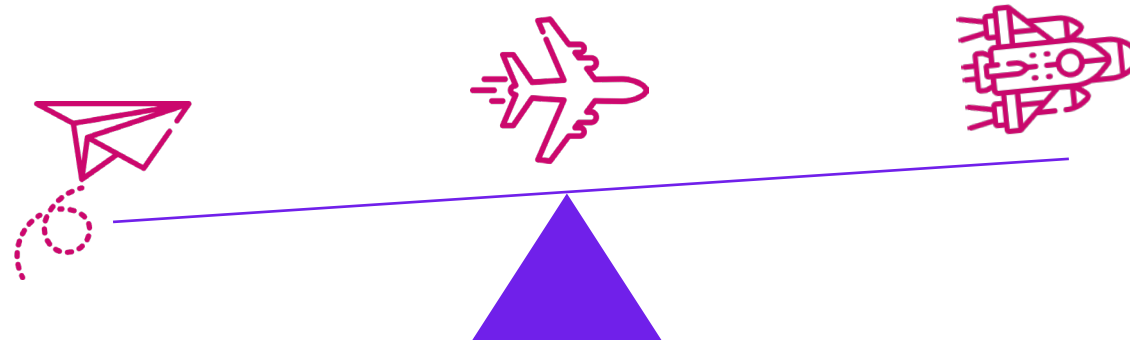
Cas d'usage



Talents &  
Expertise



Gouvernance &  
Ethique



# IA : principaux défis et risques à maîtriser pour l'audit interne

Ce que l'audit interne doit comprendre avant de pouvoir faire confiance à l'IA.

## Données & modèles (fondation)

- Données incomplètes, biaisées ou obsolètes
- Résultats non fiables ou trompeurs
- Difficulté à expliquer ou reproduire une décision

*Une IA n'est jamais meilleure que les données et les modèles qui la nourrissent*

## Gouvernance & Responsabilité

- Gouvernance IA inexistante ou floue
- Responsabilités partagées entre IT, data, business, fournisseurs
- Absence de règles claires sur les usages autorisés

*Quand tout le monde utilise l'IA, plus personne n'en est vraiment responsable*

## Dépendance et automatisation excessive

- Dépendance excessive aux outils d'IA
- Réduction de la supervision humaine
- Érosion du jugement professionnel

*Plus l'IA automatise, plus le risque de perte de contrôle augmente*

## Sécurité, conformité et tiers

- Fuites de données
- Cyberattaques spécifiques à l'IA (prompt injection, data poisoning...)
- Dépendance à des fournisseurs critiques
- Non-conformité réglementaire

*L'IA élargit la surface de risque bien au-delà des frontières de l'organisation*

## Défis clés pour l'Audit Interne

- Les risques liés à l'IA ne peuvent pas être gérés par une seule fonction
- L'audit interne joue un rôle essentiel pour structurer, challenger et renforcer la maîtrise globale



04

# Le rôle de l'Audit Interne



# Quel rôle concret pour l'audit interne face à ces défis?

De la vigilance à la création de confiance dans l'usage de l'IA.

01

## Comprendre et cadrer les usages de l'IA

On ne peut auditer que ce que l'on comprend

- Identifier où et comment l'IA est utilisée dans l'organisation
- Distinguer usages critiques vs non critiques
- Clarifier les attentes et limites de l'IA

02

## Evaluer la gouvernance et les responsabilités

Quand tout le monde utilise l'IA, quelqu'un doit en être responsable

- Clarté des rôles (business, IT, data, fournisseurs)
- Alignement avec les 3 lignes de défense
- Existence de règles, politiques, et principes d'usage

03

## Fournir une assurance indépendante sur les risques clés

L'IA change les risques, mais pas le besoin d'assurance

- Qualité des données et des modèles
- Supervision humaine et contrôles
- Sécurité, conformité et dépendances tierces

04

## Accompagner l'organisation de manière pragmatique

L'Audit Interne n'est pas un frein, mais un partenaire exigeant.

- Recommandations concrètes et prioritaires
- Sensibilisation aux risques émergents
- Contribution à une adoption responsable de l'IA

*L'audit interne ne doit pas devenir expert en IA,  
mais rester expert en risques, gouvernance et confiance*

# Jouez le rôle de conseiller de confiance, avec les deuxièmes Lignes

Une lecture pragmatique pour comprendre où l'audit interne crée le plus de valeur

Transformation des risques liés à l'IA

Surveillance des risques liés à l'IA



## Gouvernance de l'IA

Évaluer et challengez le cadres de gouvernance, les modèles opérationnels, les politiques et es procédures pour soutenir l'IA responsable.

- Cadre de gouvernance responsable de l'IA ;
- Modèle d'exploitation responsable de l'IA et matrice RACI ;
- Revue des politiques et de procédures



## Conformité à la réglementation de l'IA

Soutenez les efforts de conformité au niveau de l'organisation et du service grâce à l'évolution des réglementations en matière d'IA :

- Évaluation des lacunes en IA
- Cadre de gouvernance et de conformité de l'IA
- Classification et inventaire des systèmes d'IA
- Revue des politiques
- Soutien à l'évaluation de la conformité



## Sécurité de l'IA

- Documents de conception de haut niveau et cartes de modèle
- Inventaire des systèmes algorithmiques
- Matrice des risques et des contrôles de l'IA
- Questionnaire d'évaluation des risques liés à l'IA



## Risque et contrôle de l'IA

Évaluez et challengez les contrôles et les technologies pour intégrer l'IA dans les processus de bout en bout.

- Évaluation des risques liés à l'IA (questionnaire)
- Matrice de risques et de contrôles (ex: *Trusted AI*)
- Challengez les plans d'actions pour résoudre les préoccupations



## Validation de l'IA

Mettre à l'essai, examiner les données probantes et faire rapport sur les cadres de gestion, les processus et les contrôles relatifs à la surveillance, au développement et à l'utilisation responsables des technologies d'IA.

- Réaliser un audit interne sur les cadres de gouvernance de l'IA et le cycle de vie des cas d'utilisation de l'IA.
- Auditer le développement, le déploiement et le suivi des modèles d'IA.
- Cadrage de l'assurance IA ; Examens de diagnostics IA ; Test et attestation de contrôle du modèle d'IA

## Gestion des risques liés aux tiers



# Audit tout au long du parcours de transformation de l'IA

Pas un audit IA unique, mais des audits adaptés aux usages et aux risques

## 01 Gouvernance de l'IA

Audit du cadre de gouvernance entourant l'IA au sein de l'organisation. Audit abordant les domaines pertinents couvrant les questions clés de gouvernance, de gestion des risques et de conformité afin de contribuer à une surveillance et à une utilisation éthiques et efficaces des technologies d'IA.

**Besoins:** auditeurs ayant des connaissances en IA et en mécanismes de gouvernance avec le soutien d'auditeurs IT.

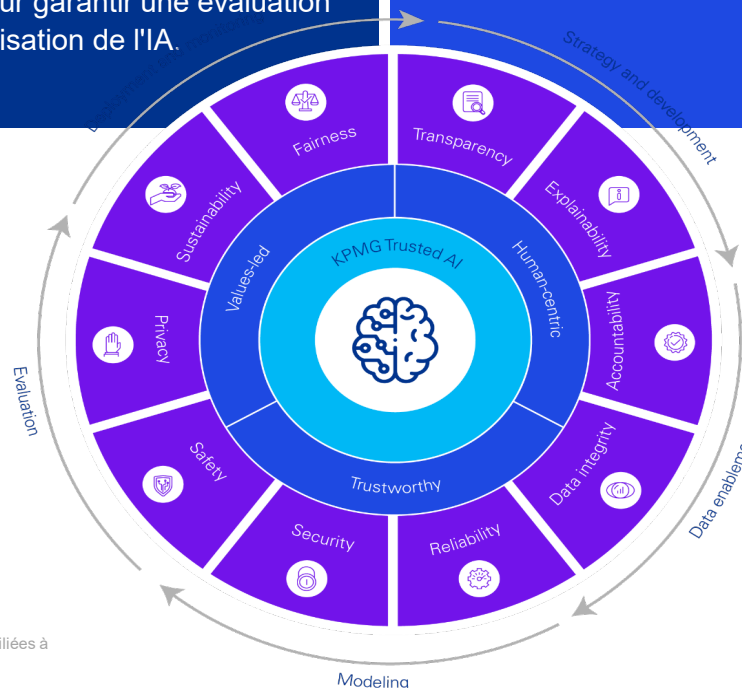
Policies & Procedures	Vision & Strategy	Governance & Oversight
AI Competences & Training	AI Landscape & Inventory	Data Management, Security & Privacy
Evaluation & Monitoring	Documentation & Record-Keeping	AI Awareness & Literacy

## 02 Cycle de vie d'un cas d'usage de l'IA

Audit sur la gestion et l'exécution des activités intégrées à l'IA au sein de l'organisation en se concentrant sur les cinq phases du cycle de vie du développement du modèle d'IA, tout en tenant compte des exigences de la loi européenne sur l'IA. Il couvre la stratégie et le développement, l'activation des données, la modélisation, l'évaluation, le déploiement et le suivi pour garantir une évaluation approfondie des cas d'utilisation de l'IA.






## 03 Audit de système d'IA

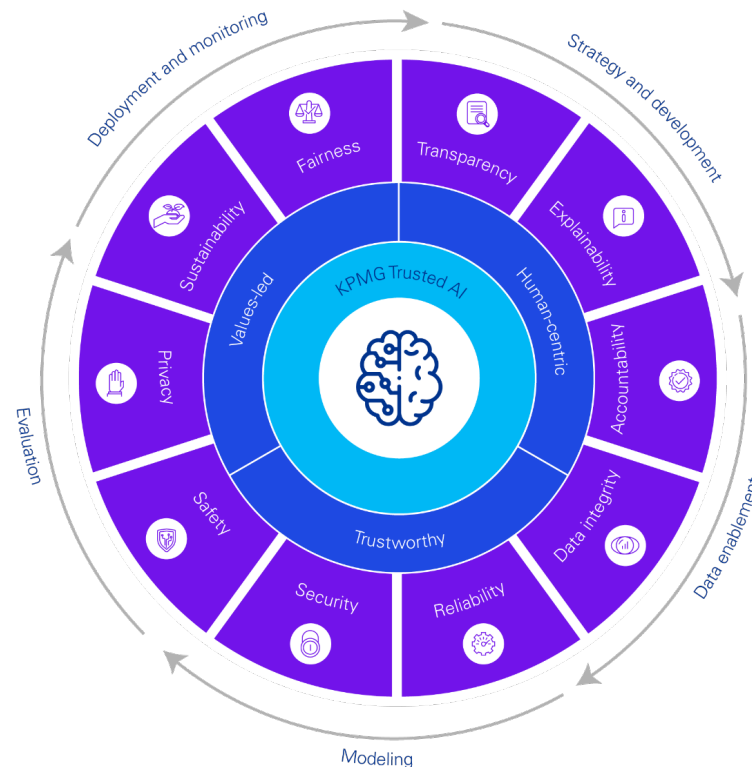
L'audit de développement, de déploiement et de suivi des systèmes d'IA se concentre sur l'évaluation des modèles d'IA de l'organisation afin d'en assurer l'exactitude, l'équité, la transparence et la conformité aux exigences réglementaires.





# Exemple : Trusted AI

	<b>Fairness</b> AI solutions should be designed to reduce or eliminate bias against individuals, communities and groups.
	<b>Transparency</b> AI solutions should include responsible disclosure to provide stakeholders with a clear understanding of what is happening in each solution across the AI lifecycle.
	<b>Explainability</b> AI solutions should be developed and delivered in a way that answers the questions of how and why a conclusion was drawn from the solution.
	<b>Accountability</b> Human oversight and responsibility should be embedded across the AI lifecycle to manage risk and comply with applicable laws and regulations.
	<b>Data integrity</b> Data used in AI solutions should be acquired in compliance with applicable laws and regulators and assessed for accuracy, completeness, appropriateness, and quality to drive trusted decisions.



	<b>Reliability</b> AI solutions should consistently operate in accordance with their intended purpose and scope and at the desired level of precision.
	<b>Security</b> Robust and resilient practices should be implemented to safeguard AI solutions against bad actors, misinformation, or adverse events.
	<b>Safety</b> AI solutions should be designed and implemented to safeguard against harm to people, businesses, and property.
	<b>Privacy</b> AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.
	<b>Sustainability</b> AI solutions should be designed to be energy efficient, reduce carbon emissions, and support a cleaner environment.



05

# Et maintenant ? Cap vers 2030

# L'auditeur de 2030

Augmenté par l'IA, mais toujours guidé par le jugement, l'indépendance et la confiance.

## ***L'auditeur interne de 2030 : traducteur de complexité et gardien du doute.***

*Il ne maîtrisera pas l'IA, mais il la challengera. Son rôle : transformer l'opacité des systèmes en questions intelligibles, identifier ce qui échappe au contrôle, et maintenir vivante la capacité de l'organisation à questionner ce qu'elle automatise. Trois piliers : indépendance du jugement, curiosité méthodique, responsabilité envers l'organisation. Plus l'IA progresse, plus son rôle devient central. (Claude AI)*

## ***L'auditeur interne de 2030 : le garant du jugement et de la confiance à l'ère de l'IA***

*L'auditeur interne de 2030 est un expert du jugement et de la confiance, capable d'analyser des environnements complexes augmentés par l'IA, de challenger les décisions et les risques, et de créer de la valeur durable pour l'organisation, tout en restant indépendant, critique et responsable de ses conclusions. (ChatGPT)*

## ***L'Auditeur Interne 2030 : Le Partenaire de Résilience Augmenté***

*En 2030, l'auditeur interne n'est plus un simple "contrôleur de conformité" a posteriori, mais un architecte de la confiance intégré au cœur de la stratégie de l'entreprise. Il combinera une maîtrise technologique avancée (data science) avec des soft skills d'influence, passant d'une fonction de "police" à celle de "phare" éclairant les décisions dans un monde complexe. (Gemini)*





Où l'IA est-elle déjà utilisée dans mon organisation... même de manière informelle ?

Quels usages de l'IA sont critiques ou sensibles du point de vue des risques ?

La gouvernance et les responsabilités autour de l'IA sont-elles claires ?

Pour quels usages l'IA crée-t-elle réellement de la valeur en audit interne aujourd'hui ?

Quels (premiers) usages concrets l'audit interne peut-il développer dès maintenant, sans augmenter inutilement les risques ?

Le rôle de l'audit interne est-il aujourd'hui suffisamment clair et positionné pour encadrer l'IA sans freiner l'innovation ?



[kpmg.com/socialmedia](https://kpmg.com/socialmedia)

© 2026 KPMG Advisory, une SRL belge et société membre de l'organisation mondiale KPMG de sociétés indépendantes affiliées à KPMG International Limited, une « private English company limited by guarantee ». Tous droits réservés.