

Étude de marché

# IA et risque cyber tiers 2026

---

Comment les entreprises  
françaises gèrent-elles  
le risque IA de leurs tiers ?

cybervadis

 CESIN

## Sommaire

### Ce que couvre l'étude

Seize sections, de la méthodologie aux leviers d'action.

### Préambule

|                         |   |
|-------------------------|---|
| Résumé exécutif         | 3 |
| Méthodologie            | 5 |
| Contexte et échantillon | 6 |

### A | IA et sécurité en interne 7

### B | Le risque IA tiers dans le TPRM 9

|                                                 |    |
|-------------------------------------------------|----|
| B.1 Cartographie des tiers et critère IA        | 11 |
| B.2 Contrôles IA dans les évaluations des tiers | 12 |
| B.3 Due diligence à base de preuves             | 14 |

### C | Visibilité sur l'usage IA des tiers 15

|                                                 |    |
|-------------------------------------------------|----|
| C.1 Shadow AI                                   | 16 |
| C.2 Agents IA autonomes des tiers               | 18 |
| C.3 Visibilité sur les sous-traitants des tiers | 19 |

### D | Clauses contractuelles IA 21

### E | Gouvernance interne du risque IA tiers 24

### Conclusion 27

### Annexe 28

## Résumé **exécutif**

83 %

des RSSI n'ont pas couvert dans leur TPRM les risques liés à l'usage de l'IA par leurs tiers.

Vous gérez probablement un risque IA tiers sans les outils pour le mesurer. Pas parce que vous avez négligé le sujet, mais parce que vos dispositifs TPRM ont été construits avant que l'IA générative ne s'installe chez vos tiers.

**Le constat est net :** 48 % des RSSI interrogés ont un processus TPRM formalisé et documenté, 26 % une démarche partielle ou informelle. Seulement 17 % déclarent que le risque IA tiers est identifié et couvert dans leur dispositif, au sens large (évaluations, cartographie, contrats, gouvernance).

Le TPRM se consolide, mais la couche IA n'y est pas encore intégrée de manière structurée. Ce n'est pas un problème de méthode : les frameworks d'évaluation des tiers existants n'ont simplement pas été mis à jour.

84 %

des RSSI n'ont pas de clause contractuelle encadrant l'usage de l'IA par leurs tiers.

68 %

des RSSI ne vérifient aucun contrôle IA chez leurs tiers.

48 %

des RSSI n'ont aucune visibilité sur l'usage de l'IA de leurs tiers.



## À retenir

Seulement 6 % des RSSI ont pleinement engagé la prise en compte de l'IA dans le TPRM et cumulent les trois pratiques : l'usage de l'IA reclassifie la criticité de tiers, des contrôles IA figurent dans les évaluations, des clauses IA dans les contrats. Ils restent rares mais le chemin est tracé.

Votre visibilité est plafonnée par la maturité de votre tiers : seulement 4 % des tiers prouvent tenir un inventaire de leurs propres outils IA, alors que 65 % le déclarent.

Les **quatre leviers** sont connus, arbitrés en conclusion et repris en annexe :

1

Un critère IA dans la grille de criticité (B.1)

2

Des contrôles IA vérifiés sur preuves dans les évaluations des tiers (B.2, B.3)

3

Des clauses IA dans les contrats, jusqu'au rang N+2 (D)

4

Une gouvernance transverse pour piloter l'ensemble (E)

Aucun ne demande de refonte : ce sont des mises à jour du dispositif existant.

Un chantier distinct mérite une vigilance propre : les agents IA autonomes de vos tiers, qui agissent sans validation humaine et posent trois questions spécifiques, traçabilité, périmètre d'accès et imputabilité, détaillées en section C.2.

# Méthodologie

Cette étude croise deux sources de données complémentaires : une enquête déclarative menée auprès des membres du CESIN, et les évaluations cyber tierces conduites par CyberVadis sur preuves documentaires.

L'enquête CESIN a été conduite auprès de 111 membres du CESIN, RSSI d'entreprises françaises gérant un périmètre tiers actif, entre mai et juin 2026. Le questionnaire, auto-administré en ligne avec garantie d'anonymat, couvre les pratiques TPRM (Third-Party Risk Management, soit la gestion du risque cyber posé par les tiers : fournisseurs, prestataires et sous-traitants), la perception du risque IA tiers, et les dispositifs de gouvernance.

Les réponses ont été traitées de manière strictement agrégée. Les 111 répondants n'ont pas tous complété chaque bloc du questionnaire : l'effectif utile varie donc selon les questions, et il est précisé (n=) avec chaque résultat. Les répondants exercent majoritairement des fonctions de RSSI (87 %) au sein d'ETI et grandes entreprises (80 %).



## Enquête CESIN

Perceptions et pratiques TPRM déclarées par 111 membres du CESIN, base principale de l'analyse. Biais : population de RSSI sensibilisés et structurés, susceptible de surestimer la maturité moyenne du marché. Sous-segments avec n < 10 non publiés ; bases variables selon les questions (n = 85 à 111).



## Données CyberVadis

Évaluations cyber tierces conduites par CyberVadis depuis janvier 2025 : 652 évaluations, dans 49 pays, 6 contrôles IA spécifiques évalués avec revue documentaire. Une réponse n'est considérée comme démontrée que si elle est étayée par des preuves de définition et d'implémentation.

Les deux sources ne portent pas sur les mêmes organisations : les 652 tiers évalués ne sont pas les fournisseurs des 111 RSSI interrogés. Les rapprochements entre les deux volets sont structurels, pas un appariement client-fournisseur.

Les chiffres marqués d'un astérisque dans ce rapport ne se lisent pas dans un graphique : ils résultent du croisement de deux questions de l'enquête. La sous-population concernée est précisée à chaque fois.

# Contexte et échantillon

L'enquête a été conduite auprès de 111 RSSI membres du CESIN entre mai et juin 2026. L'échantillon couvre majoritairement des ETI et grandes entreprises, dans une diversité de secteurs et de niveaux d'exposition réglementaire.

**111**

répondants RSSI  
membres du CESIN.

**87 %**

exercent une fonction  
de RSSI.

**55 %**

sont soumis à NIS2.

## Taille des organisations

Grande entreprise  
(>5000 ETP)

**33 %**

ETI (250-4999 ETP)

**47 %**

TPE/PME (<250 ETP)

**20 %**

## Secteurs principaux

Information et communication

**24 %**

Finance et assurance

**17 %**

Industrie

**15 %**

Santé

**8 %**



A

---

IA et sécurité  
en interne

# L'IA s'installe vite, la gouvernance sécurité reste à la traîne

45 %

des RSSI ont intégré l'IA dans leur stratégie de sécurité, en hausse de 10 points (35 % en 2025).

## Quelle place occupe l'IA dans votre organisation ?

IA intégrée dans la stratégie de sécurité

45 %

IA utilisée officiellement,  
sans stratégie sécurité

40 %

Usage IA non officiel (Shadow AI)

11 %

IA pas encore utilisée

4 %

Le verre est à moitié plein : 45 % ont adapté leur stratégie de sécurité. La dynamique est réelle. Mais 40 % naviguent encore sans filet : IA déployée, gouvernance sécurité absente. Fait révélateur : presque la moitié des organisations qui ont intégré l'IA dans leur stratégie de sécurité interne ne vérifient pourtant aucun contrôle IA chez leurs tiers<sup>1</sup>.

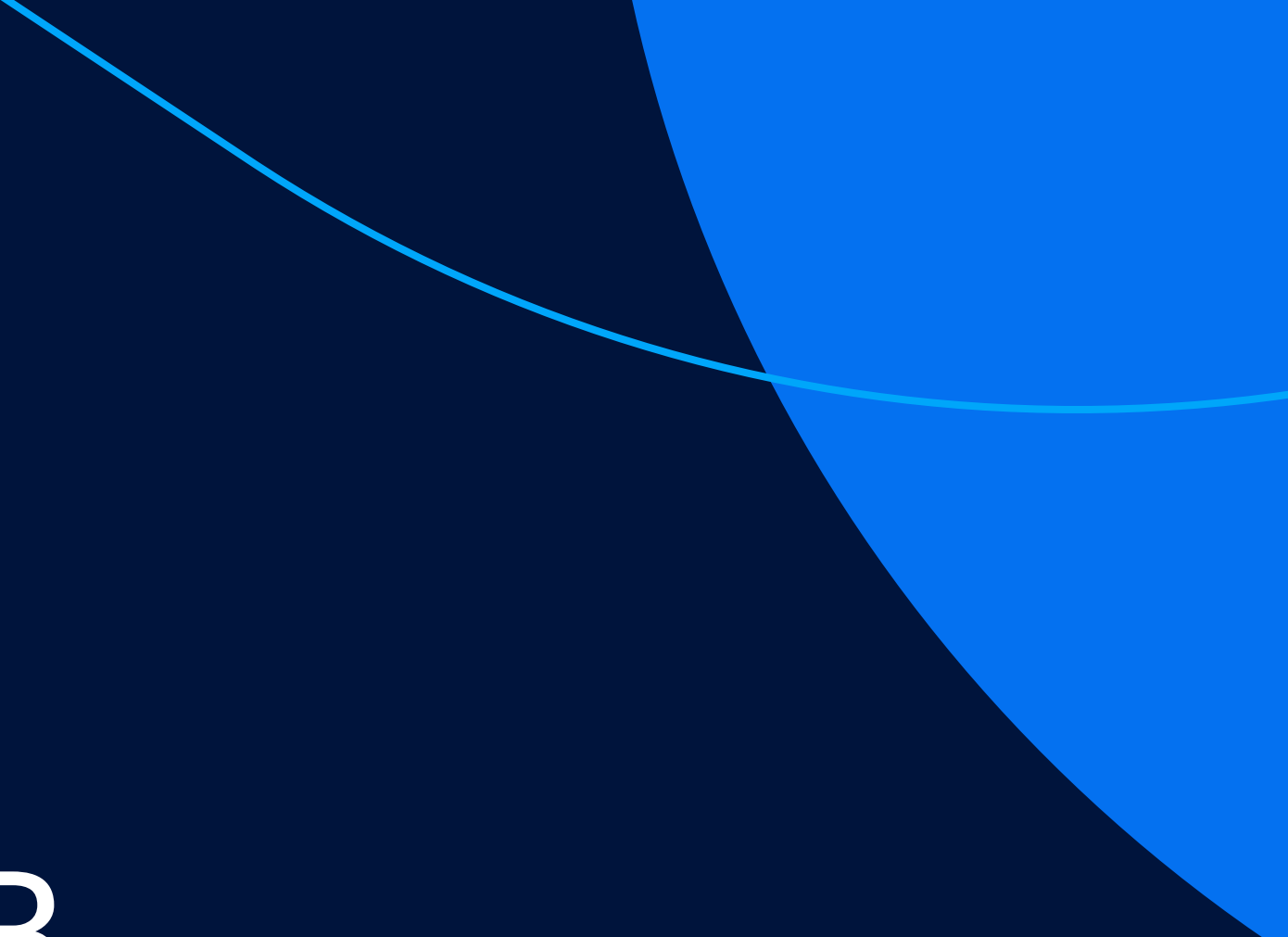
C'est le même phénomène qui se rejoue en chaîne : le Shadow AI que 11 % des organisations tolèrent en interne a son miroir chez les tiers, le « Shadow AI Supplier » développé en [C.1](#), une IA que le tiers utilise ouvertement, mais que vous ne voyez pas.



## Données CyberVadis

Seulement 4 % des tiers évalués parviennent à démontrer après revue documentaire qu'ils tiennent un inventaire de leurs outils IA. Le retard de gouvernance IA en interne, observé chez les RSSI répondants au sondage, se retrouve accentué côté tiers.

<sup>1</sup> Croisement de la place de l'IA en interne et des contrôles IA vérifiés. Sous-population : les 45 % ayant intégré l'IA dans leur stratégie.



B

---

Le risque IA tiers  
dans le TPRM

## Le TPRM se consolide, mais la variable IA n'y est pas encore prise en compte

48 %

des RSSI ont un processus TPRM formalisé et documenté : le dispositif se consolide, il n'est pas généralisé.

**Votre organisation dispose-t-elle d'un processus formalisé d'évaluation du risque cyber de ses fournisseurs critiques ? (n=92)**

Oui, processus formalisé et documenté

48 %

Oui, mais partiel ou informel

26 %

Non, structuration prévue sous 12 mois

18 %

Non, pas encore

8 %

Un processus partiel ou informel n'a ni périmètre stable, ni répétabilité, ni preuve. La variable IA arrive donc sur des fondations qui, pour un RSSI sur deux, restent à structurer.

83 %

des RSSI n'ont pas couvert dans leur TPRM les risques liés à l'usage de l'IA par leurs tiers.

**Comment les RSSI perçoivent-ils le risque IA dans leur TPRM ?**

Identifié et couvert dans le TPRM

17 %

Identifié mais pas évalué

46 %

Pas clairement identifié

30 %

Impossible à évaluer

7 %

Les RSSI voient le risque : la conscience est là. Ce qui manque, c'est le passage à l'acte, détaillé dans les sections suivantes : la cartographie ([B.1](#)), les contrôles vérifiés dans les évaluations ([B.2](#)), la due diligence sur preuves ([B.3](#)).

# La cartographie des tiers existe, mais l'usage de l'IA ne pèse pas encore dans l'évaluation de leur criticité

**65 %**

des organisations disposent déjà d'une cartographie des tiers (complète ou partielle par criticité cyber).

## Disposez-vous d'une cartographie des tiers par criticité cyber ?

Complète et à jour

22 %

Partielle : tiers critiques seulement

43 %

Prévue dans les 12 prochains mois

22 %

Pas de cartographie formalisée

13 %

## L'IA modifie-t-elle votre façon d'évaluer la criticité d'un tiers ?

Formalisé dans la grille de criticité

5 %

Informellement, selon le contexte

18 %

Mise à jour prévue dans 12 mois

34 %

Grille non mise à jour

43 %



### À retenir

Le chantier le plus rapide: ajouter un critère IA binaire, « ce tiers utilise-t-il l'IA pour traiter nos données ou livrer notre service ? ». Un oui rehausse le niveau de criticité et déclenche une évaluation approfondie. Une mise à jour, pas une refonte.

# Les contrôles IA restent rarement vérifiés dans les évaluations des tiers

**68 %**

des RSSI ne vérifient aucun contrôle IA spécifique dans leurs évaluations des tiers.

**Quels contrôles spécifiques à l'IA vérifiez-vous dans vos évaluations des tiers? (plusieurs choix possibles)**

Aucun contrôle IA spécifique

68 %

Protection des données dans les modèles IA

20 %

Analyse de risque IA spécifique

17 %

Inventaire des outils et systèmes IA

14 %

Contrôle de l'usage des données par modèles IA tiers

14 %

Formation des équipes au risque IA

11 %

Six contrôles structurent la due diligence IA d'un tiers. L'enquête CESIN couvre les cinq premiers; le sixième, le cadre réglementaire, est mesuré côté tiers dans les évaluations CyberVadis ([section B.3](#)). Pour la mise en œuvre, l'ANSSI a publié les « Recommandations de sécurité pour un système d'IA générative » (ANSSI-PA-102, avril 2024).

## NIS2 et AI Act : anticipation plus que conformité

Le dispositif TPRM existe, mais un RSSI sur deux seulement l'a formalisé : 48 % ont un processus formalisé et documenté, 26 % une démarche partielle ou informelle. L'IA n'y est pas intégrée : 68 % ne vérifient aucun contrôle IA spécifique, et la minorité qui le fait (32 %) reste fragmentée. Le gap n'est pas un défaut de méthode : les frameworks ont été conçus avant l'IA générative.

Point de vigilance NIS2 : 65 % des entités essentielles ne vérifient aucun contrôle IA dans leurs évaluations des tiers<sup>1</sup>, quasiment identique aux 68 % de l'échantillon complet. NIS2 impose de maîtriser le risque de la chaîne d'approvisionnement (article 21) sans exigence IA explicite. La pression réglementaire dédiée viendra de l'AI Act, qui encadrera les systèmes à haut risque à partir de décembre 2027.



### Calendrier AI Act · à retenir

Pratiques interdites depuis le 2 février 2025, obligations pour les modèles d'IA à usage général depuis le 2 août 2025, pouvoirs de sanction complets de la Commission à partir du 2 août 2026, et obligations spécifiques aux systèmes à haut risque (annexe III) reportées au 2 décembre 2027 par l'accord Digital Omnibus du 7 mai 2026.

Le texte a été définitivement adopté (Parlement le 16 juin, Conseil le 29 juin 2026) ; pour l'IA à haut risque embarquée dans des produits réglementés (annexe I), l'échéance est portée au 2 août 2028.

Vérifier ces contrôles aujourd'hui relève donc de l'anticipation et de la gestion de risque plus que d'une exigence de conformité formelle.

<sup>1</sup> Croisement du statwtes contrôles IA vérifiés. Sous-population : les 28 % déclarés entités essentielles.

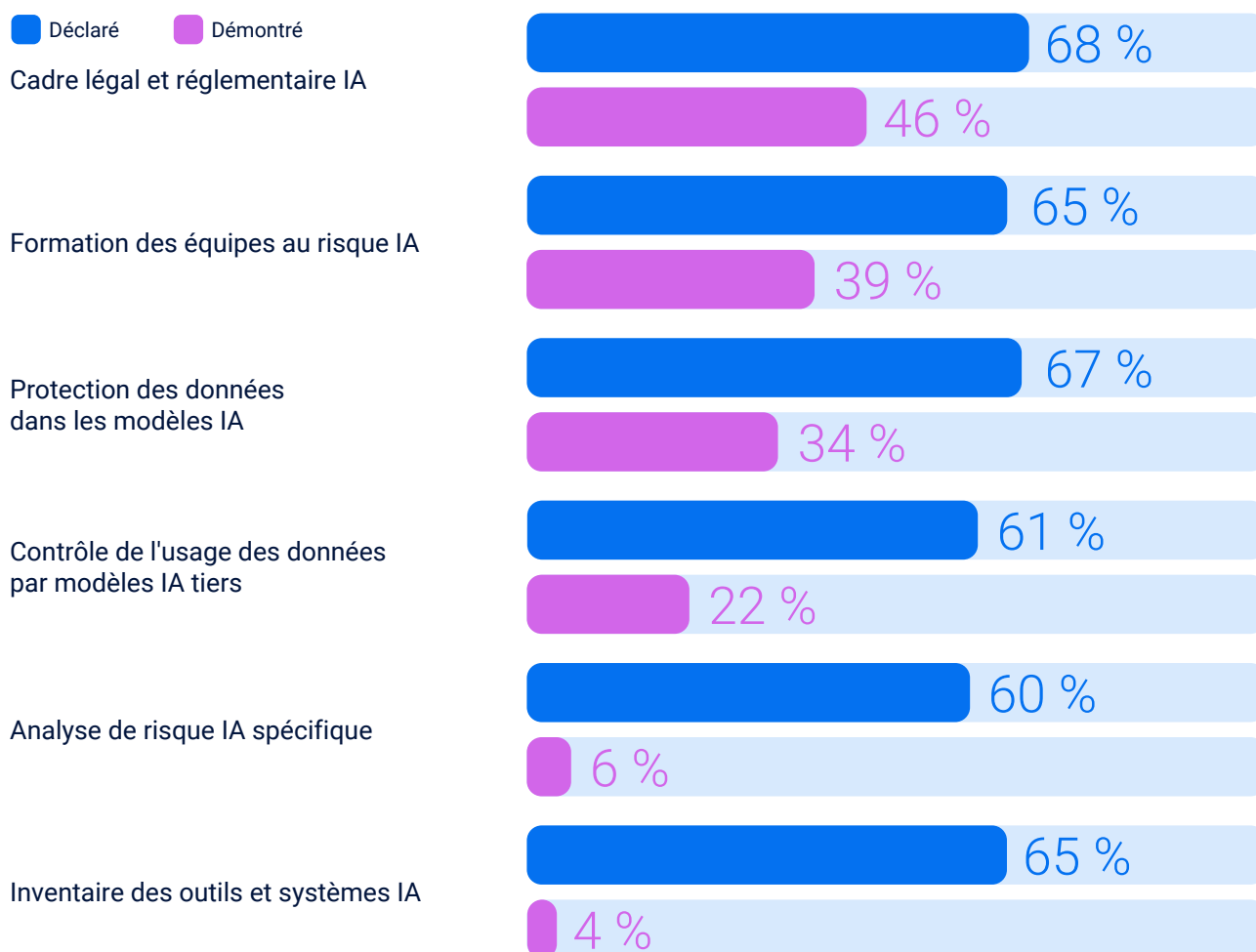
# Sur preuves, une déclaration sur deux ne tient pas

**50 %**

des déclarations « oui » des tiers sur les contrôles IA ne sont pas soutenues par des preuves suffisantes.

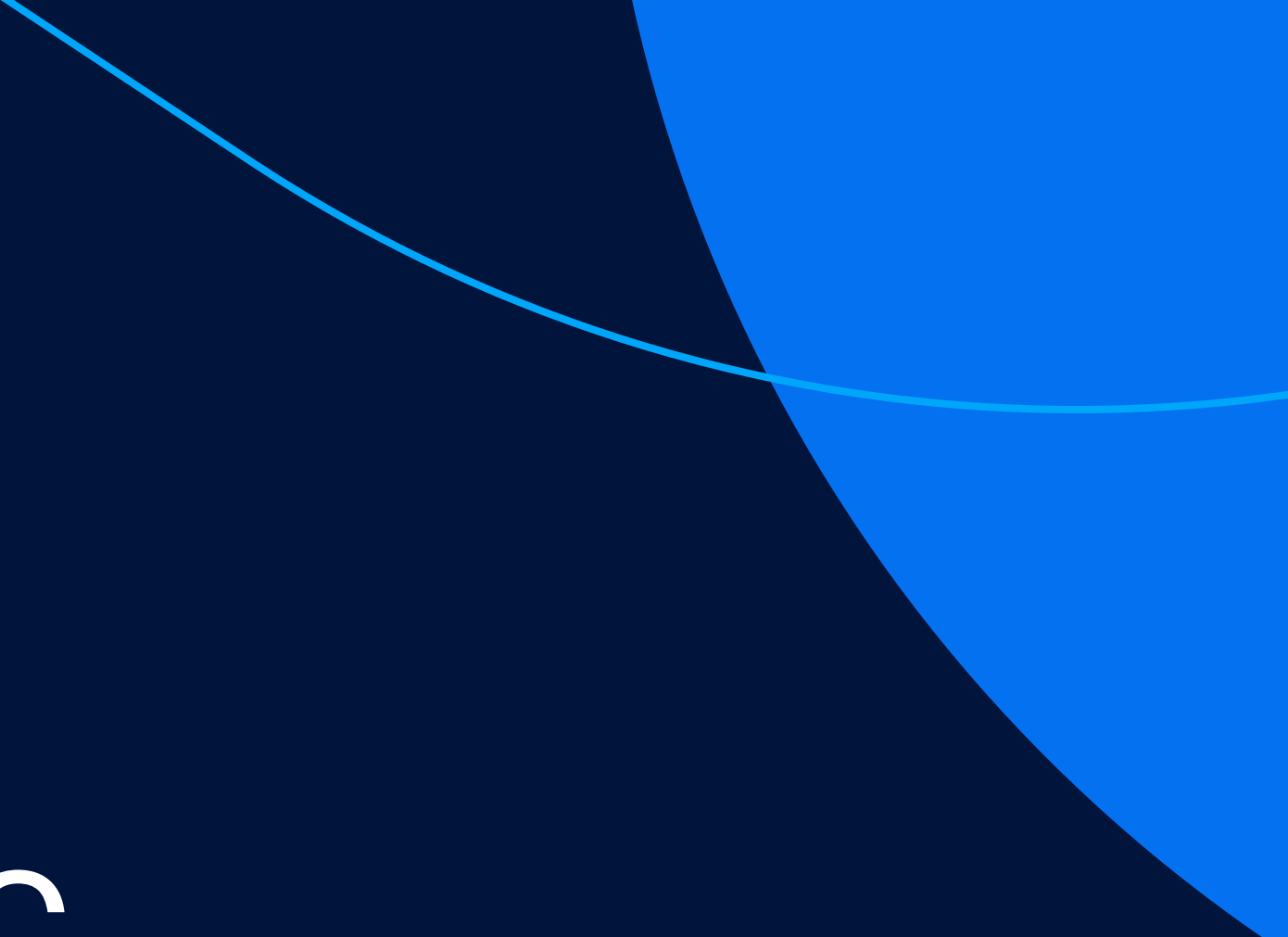
CyberVadis évalue depuis janvier 2025 la maturité IA des tiers dans le cadre de ses évaluations tierces, dans 49 pays. En moyenne, seul 1,5 contrôle sur 6 est effectivement démontré.

## Les 6 contrôles IA : ce que les tiers déclarent, ce qu'ils démontrent (n = 652)



## Données CyberVadis

Les 11 tiers (sur 652 évaluations) qui valident les 6 contrôles IA sur preuves sont avant tout des organisations dont la posture cybersécurité globale est déjà mature : score moyen 910/1000, aucun sous 750, 9 sur 11 classés « Mature ». L'IA n'a pas sa propre trajectoire, elle suit celle du socle cyber existant.



C

---

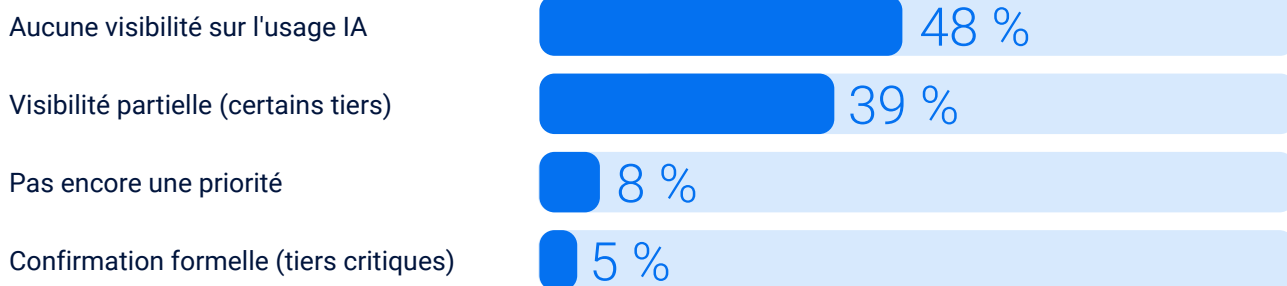
Visibilité sur l'usage  
IA des tiers

# Shadow AI Supplier: l'IA officielle des tiers, invisible pour leurs clients

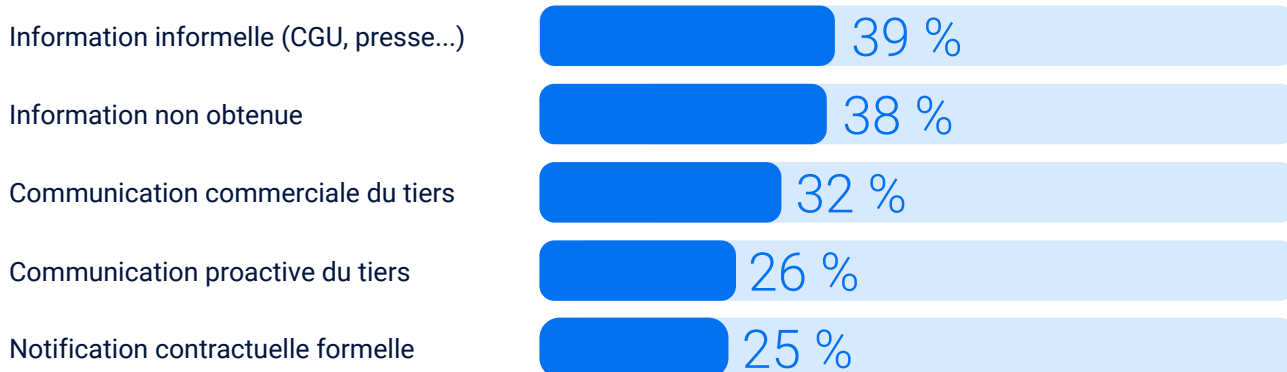
**48 %** | des RSSI n'ont aucune visibilité sur l'usage de l'IA par leurs tiers.

Le terme ne désigne pas une IA clandestine. Il s'agit d'une IA que les tiers déploient de manière parfaitement assumée pour traiter les données de leurs clients, mais dont ces derniers n'ont aucune visibilité

## Savez-vous si vos tiers utilisent l'IA pour traiter vos données ?



## Par quel canal apprenez-vous l'usage IA de vos tiers ? (plusieurs choix)



39 % obtiennent l'information de manière informelle, 38 % ne l'obtiennent pas du tout. Les canaux informels signalent un usage de l'IA sans le confirmer : à traiter comme un déclencheur de due diligence, pas comme une confirmation. Parmi les canaux observés, la notification contractuelle (25 %) est le seul opposable, là où elle existe.

## Le double angle mort de la visibilité



### Données CyberVadis

Seulement 22 % des tiers évalués démontrent après revue documentaire qu'ils contrôlent l'usage de vos données dans leurs modèles IA tiers. Quand vos tiers utilisent ChatGPT sur vos données, 78 % ne peuvent pas prouver qu'ils le maîtrisent. Côté RSSI, 48 % n'ont aucune visibilité sur l'usage IA de leurs tiers ; côté tiers, seulement 4 % démontrent tenir un inventaire de leurs propres outils IA. Vous ne pouvez pas voir ce que votre tiers ne sait pas lui-même.



### ISO/IEC 42001 : 2023 · à noter

Première norme internationale certifiable dédiée au management de l'IA. Son adoption reste embryonnaire : l'exiger aujourd'hui en clause éliminatoire reviendrait à exclure la quasi-totalité du panel fournisseurs. Tant que la réglementation n'oblige pas, la preuve documentaire reste le seul élément vérifiable.

# Les agents IA autonomes des tiers, la zone d'ombre de demain

**27 %**

des RSSI ne savent pas si leurs tiers déploient des agents IA autonomes, et n'ont alors aucun contrôle IA dans leurs évaluations\*.

## Savez-vous si vos tiers utilisent l'IA pour traiter vos données ?

Non, pas à notre connaissance

**53 %**Nous ne savons pas  
(point d'incertitude)**27 %**

Oui, mais usage non encadré

**7 %**Oui, cadre de gouvernance prévu  
sous 12 mois**7 %**Oui, avec un cadre  
de gouvernance défini**6 %**

Un agent IA ne se contente plus de répondre : il agit. Il enchaîne des actions sans validation humaine, accéder à des systèmes, modifier des données, déclencher des transactions, produire et exécuter du code. La traçabilité des actions, le périmètre d'accès et l'imputabilité en cas d'incident deviennent les trois questions centrales.

\* Croisement du statut NIS2 et des contrôles IA vérifiés. Sous-population : les 28 % déclarés entités essentielles.

---

## Par où commencer

### Trois exigences spécifiques aux agents IA tiers

**1**

#### Traçabilité

Exiger un journal d'audit horodaté de chaque action de l'agent (accès, modification, transaction), restituable à votre demande sous un délai défini contractuellement. L'exigence porte sur un extrait exploitable en cas d'incident, pas seulement sur des journaux internes au tiers.

**2**

#### Périmètre d'accès

Imposer le principe du moindre privilège (l'agent n'accède qu'aux systèmes et données strictement nécessaires à sa tâche) et un mécanisme de coupure immédiate que vous pouvez actionner sans délai de préavis contractuel.

**3**

#### Imputabilité

Clarifier par contrat, avant l'incident et non pendant, qui répond d'une action dommageable de l'agent : le tiers qui l'exploite, l'éditeur du modèle sous-jacent, ou une responsabilité partagée selon la nature de l'action.

Ces exigences complètent les cinq clauses IA générales ([section D](#)) sans les remplacer : un agent autonome engage une action, pas un simple traitement de données. L'incertitude sur les agents IA est un marqueur d'absence totale de dispositif : les organisations qui ne savent pas si leurs tiers en déploient n'ont, dans 100 % des cas, aucun contrôle IA en place ailleurs dans leur TPRM.

## Au rang N+2, l'angle mort devient total

**89 %**

des RSSI n'ont aucune visibilité sur l'usage de l'IA par les sous-traitants de leurs tiers directs.

### Avez-vous une visibilité sur l'usage de l'IA par les sous-traitants de vos fournisseurs directs (4th parties) ?

TPRM couvre explicitement le niveau N+2

**2 %**

Partielle (tiers critiques seulement)

**9 %**

Périmètre limité aux tiers directs (N+1)

**46 %**

Aucune visibilité, sujet non adressé

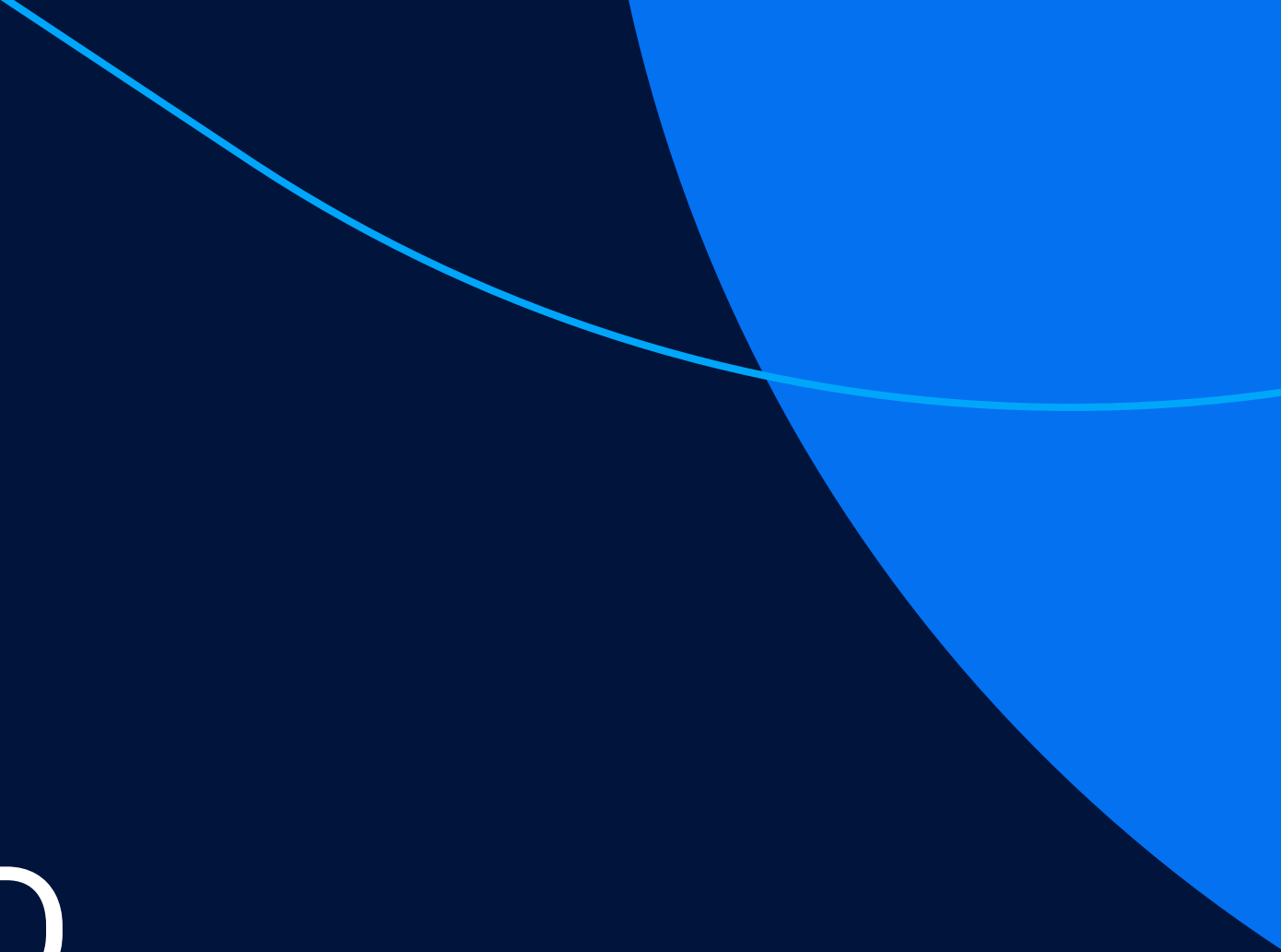
**43 %**

2 % des répondants couvrent le niveau N+2 dans leur TPRM. Seul levier direct: obliger contractuellement le tiers à répercuter les exigences IA à ses propres sous-traitants.



### À retenir

L'angle mort N+2 n'est pas un détail de périmètre: c'est la zone où vos données circulent sans qu'aucun de vos contrôles ne s'applique. La répercussion en chaîne détaillée en section D est la réponse la plus pragmatique.



D

---

Clauses  
contractuelles IA

## L'élan contractuel est réel, le cadre reste à poser

84 %

des RSSI n'ont pas de clause contractuelle encadrant l'usage de l'IA par leurs tiers.

Le contrat est le premier levier opposable dont dispose un donneur d'ordre. Une clause IA peut s'adosser à une charte ou politique IA annexée au contrat : vos exigences internes deviennent alors des engagements du tiers.

### Vos contrats tiers encadrent-ils spécifiquement l'usage de l'IA ?

Oui, de manière systématique

9 %

Oui, sur certains contrats ciblés

7 %

Chantier ouvert, échéance  
dans 12 mois

44 %

Non, sans ressources pour rédiger

11 %

Non, sans échéance définie

29 %



### Données CyberVadis

Une clause IA efficace suppose que le tiers sache quels outils IA il utilise. Seulement 4 % le démontrent après revue documentaire. La clause est une condition nécessaire, pas suffisante.

---

## Par où commencer

### Cinq clauses incontournables

1

#### Interdiction d'entraînement

Vos données ne servent pas à entraîner ou ré-entraîner des modèles IA sans accord explicite. La clause la plus répandue du marché.

2

#### Notification

Le tiers déclare tout usage d'IA sur vos données, existant ou nouveau.

3

#### Déclaration des modèles et sous-traitants IA

La liste des systèmes et prestataires IA mobilisés sur votre périmètre, tenue à jour.

4

#### Droit d'audit de l'usage IA

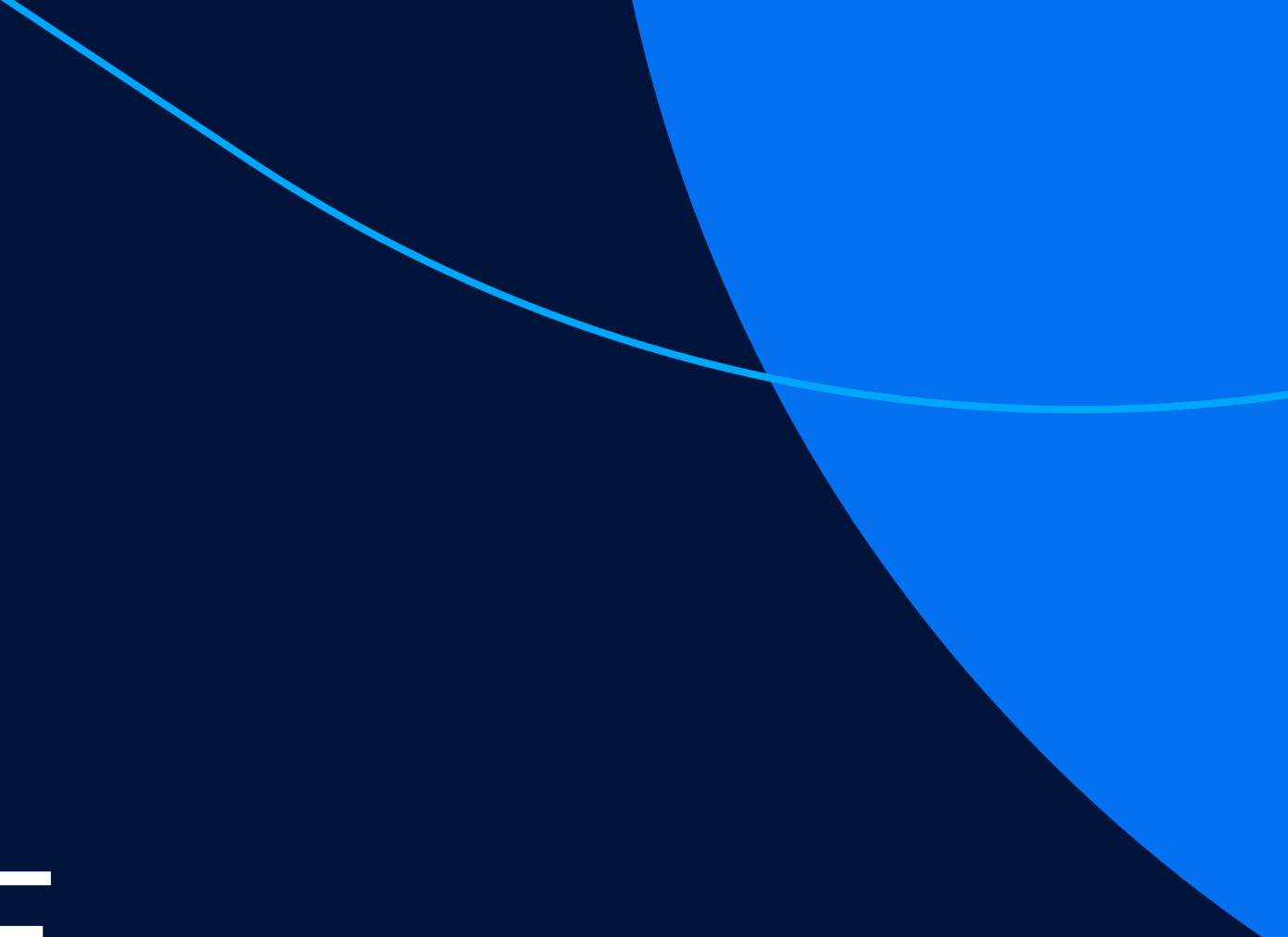
Revue documentaire ou évaluation indépendante, à votre demande.

5

#### Répercussion en chaîne

Le tiers impose ces mêmes exigences à ses propres sous-traitants IA (rang N+2).

Point d'appui pour les formulations : les clauses types MCC-AI (Public Buyers Community, mars 2025, disponibles en français), alignées sur l'AI Act. Conçues pour l'achat d'un système d'IA, elles ne couvrent pas la notification d'un usage IA dans un service qui n'en est pas un.



E

---

Gouvernance interne  
du risque IA tiers

# Le risque IA tiers est porté en interne, la coordination reste à construire

**48 %**

des RSSI ont identifié la Direction cybersécurité comme propriétaire du risque IA tiers : un premier ancrage.

Le risque IA tiers est par nature transverse : sécurité des SI, protection des données, relations contractuelles, conformité (RGPD, AI Act). Une vulnérabilité dans l'outil IA d'un tiers peut devenir un point d'entrée sur votre propre système d'information.

## Qui dans votre organisation est propriétaire du risque IA tiers ?

Direction cybersécurité (seule)

48 %

Pas de propriétaire identifié

25 %

Responsabilité partagée  
non coordonnée

16 %

Direction juridique

5 %

Comité transverse formalisé

4 %

Direction achats

2 %



### À retenir

Seulement 4 % ont un comité transverse formalisé. Le schéma le plus complet observé associe la Direction cybersécurité comme point d'ancrage, le juridique pour les clauses et les achats pour les renouvellements. Il reste à le formaliser.

---

## Par où commencer

### Quatre briques de gouvernance IA

1

#### Une politique IA formalisée

Couvrant les usages internes comme ceux des tiers : le document de référence que la clause contractuelle pourra ensuite opposer.

2

#### Un inventaire des usages IA

Outils internes, IA embarquée chez les tiers, agents autonomes. On ne gouverne pas ce qu'on ne voit pas.

3

#### Un comité transverse

Cybersécurité, juridique, achats, métiers : chaque direction tient un morceau du risque, aucune ne le couvre seule.

4

#### L'intégration au TPRM existant

Critère IA dans la grille de criticité, contrôles IA dans les évaluations, clause de notification dans les contrats.

## Trois priorités pour passer à l'action

6 %

des RSSI cumulent déjà les trois pratiques : criticité, contrôles, clauses. Ils sont rares, mais le chemin est tracé.

Les données de cette étude décrivent une transition, pas une rupture. Les organisations françaises sont en cours d'implémentation de leurs dispositifs TPRM ; ce qu'elles n'ont pas encore fait, c'est l'enrichir de la variable IA. C'est une mise à jour, pas une reconstruction. Ces trois priorités regroupent les quatre leviers. Les agents IA restent un chantier distinct (C.2).

1

### Mettre à jour les frameworks TPRM

Ajouter un critère IA binaire dans la grille de criticité et intégrer les six contrôles de la due diligence IA dans les évaluations des tiers (sections [B.1](#) à [B.3](#)).

2

### Contractualiser la transparence

Intégrer les cinq clauses détaillées en [section D](#). Les clauses types MCC-AI (mars 2025) donnent la structure pour l'achat de systèmes d'IA. 44 % ont déjà ce chantier ouvert

3

### Formaliser la gouvernance transverse

La Direction cybersécurité comme point d'ancrage, en coordination avec le juridique et les achats, dans un comité transverse formalisé ([section E](#)).

# Check-list opérationnelle

Les quatre leviers du rapport, en questions, puis un scénario de mise en route.

## Auto-diagnostic express : où vous situez-vous ?



1. Le critère IA est-il intégré à votre grille de criticité des tiers ? (B.1)
2. Vérifiez-vous les six contrôles IA sur preuves dans vos évaluations ? (B.2, B.3)
3. Vos contrats comportent-ils les cinq clauses IA, jusqu'au rang N+2 ? (D)
4. Un comité transverse cyber, juridique et achats suit-il le sujet ? (E)

Quatre « oui » signalent un dispositif complet. Un chantier reste hors de cette grille : les agents IA autonomes de vos tiers (C.2). Pour référence, 6 % des RSSI cumulent aujourd'hui les trois pratiques de criticité, contrôles et clauses.



## Scénario illustratif · cas fictif

Une ETI du secteur assurance, via l'auto-diagnostic ci-dessus, ne coche aucun des quatre critères : la Direction cybersécurité est identifiée comme propriétaire du sujet, mais sans comité transverse ni intégration au TPRM

### Trajectoire · Trois mois pour amorcer la démarche

**Mois 1 :** elle formalise une politique IA d'une page et lance l'inventaire de ses tiers utilisant l'IA à partir des 20 contrats les plus critiques.

**Mois 2 :** elle ajoute la question binaire de criticité IA à sa grille d'évaluation des tiers et intègre une clause de notification dans les deux contrats en cours de renouvellement.

**Mois 3 :** elle réunit pour la première fois cybersécurité, juridique et achats en comité informel pour arbitrer les tiers à rebasculer en évaluation approfondie.

Elle ne repart pas de zéro et n'attend pas d'avoir un dispositif complet pour commencer : elle enrichit son TPRM existant, brique par brique, avec les ressources d'une équipe cyber ordinaire.