

L'IA se diffuse dans la chaîne de fournisseurs plus vite que les organisations n'arrivent à en maîtriser les usages, révèle une étude CyberVadis x CESIN

83 % des RSSI n'ont pas encore intégré ce risque à leur dispositif de gestion des tiers : une étude inédite menée auprès de 111 RSSI et croisée avec 652 évaluations tierces sur preuves dans 49 pays met au jour un angle mort partagé entre donneurs d'ordre et fournisseurs

Paris, le 21 septembre 2026. CyberVadis, plateforme SaaS d'évaluation du risque cyber des tiers, et le CESIN, association des experts de la sécurité de l'information et du numérique, publient aujourd'hui « *IA et risque cyber tiers 2026* », une étude qui croise pour la première fois la perception des RSSI français avec des données de terrain issues d'évaluations conduites sur preuves documentaires.

Le constat dépasse le seul périmètre de la sécurité : l'IA se diffuse dans les usages des fournisseurs plus vite que les organisations, donneurs d'ordre comme tiers, n'arrivent à en cadrer l'usage. Il ne s'agit pas d'une impréparation des RSSI, mais d'un nouvel angle mort qui se développe à grande vitesse dans l'écosystème des tiers, un sujet qui engage autant la cybersécurité que les achats, le juridique et la gouvernance des organisations.

Les chiffres clés de l'étude

- 83 % des RSSI n'ont pas couvert dans leur TPRM les risques liés à l'usage de l'IA par leurs tiers, et 68 % ne vérifient aucun contrôle IA spécifique lors des évaluations.
- 84 % n'ont pas de clause contractuelle encadrant l'usage de l'IA par leurs fournisseurs.
- 48 % des RSSI n'ont aucune visibilité sur l'usage de l'IA par leurs tiers ; 89 % n'en ont aucune sur les sous-traitants de leurs tiers (rang N+2).
- Côté preuve : seuls 4 % des tiers évalués par CyberVadis démontrent tenir un inventaire de leurs outils IA, alors que 65 % le déclarent. En moyenne, seul 1,5 contrôle IA sur 6 est effectivement démontré sur les 652 évaluations analysées.
- Seulement 6 % des RSSI ont pleinement engagé la prise en compte de l'IA dans leur TPRM : un critère de criticité IA, des contrôles IA dans les évaluations, et des clauses IA dans les contrats.

Un angle mort partagé, qui commence dès le premier rang de sous-traitance

Menée entre mai et juin 2026 auprès de 111 RSSI membres du CESIN, l'enquête est mise en regard des évaluations cyber tierces conduites par CyberVadis depuis janvier 2025 : 652 évaluations dans 49 pays, incluant six contrôles IA spécifiques vérifiés sur preuves documentaires. Cette double lecture, déclarative et vérifiée, permet de mesurer l'écart entre ce que les fournisseurs affirment et ce qu'ils démontrent réellement.

L'étude documente notamment le phénomène du « Shadow AI Supplier » : une IA que le tiers déploie ouvertement pour traiter les données de ses clients, mais dont ces derniers n'ont aucune visibilité faute de canal formel pour en être informés. Elle consacre également une section aux agents IA autonomes déployés par les tiers, qui posent des enjeux spécifiques de traçabilité, de périmètre d'accès et d'imputabilité en cas d'incident.

Une étude, quatre leviers d'action

Au-delà du diagnostic, l'étude détaille en conclusion quatre leviers, qui ne relèvent pas de la seule cybersécurité : un critère IA dans la grille de criticité, des contrôles IA vérifiés sur preuves dans les évaluations, des clauses IA dans les contrats, et une gouvernance transverse pour piloter l'ensemble, associant cybersécurité, juridique et achats. Aucun de ces leviers n'exige de remise en cause en profondeur du TPRM, il s'agit juste de mettre à jour le dispositif existant.

« Les fondations du TPRM sont solides, la couche IA doit désormais s'y intégrer, ce n'est pas une refonte mais une mise à jour. »

Thibault Lapédagne, VP Research, CyberVadis, co-auteur de l'étude

« Le risque IA ne s'arrête pas aux frontières de l'entreprise. Il s'étend à toute la chaîne de fournisseurs, alors même que la visibilité diminue à chaque niveau de sous-traitance. »

Alain Bouillé, Délégué Général du CESIN

Disponibilité et rendez-vous

- L'étude complète « IA et risque cyber tiers 2026 » est disponible en téléchargement sur cybervadis.com à compter du 21 septembre 2026.
- Un webinaire de présentation des résultats se tiendra le 2 octobre 2026.
- CyberVadis et le CESIN seront présents aux Assises de la Cybersécurité, du 7 au 9 octobre 2026 à Monaco, où les participants pourront échanger sur les enseignements de l'étude directement sur leurs stands respectifs.

À propos de CyberVadis

CyberVadis est une plateforme SaaS dédiée à l'évaluation du risque cyber des tiers (TPRM). Sa mission : aider les organisations à sécuriser leur écosystème en évaluant les risques cyber de leurs tiers de manière plus intelligente, plus rapide et plus fiable, sur la base de preuves vérifiées par des analystes plutôt que de déclarations non contrôlées.

Chaque évaluation repose sur des preuves documentaires de conception et de mise en œuvre, revues par des analystes humains selon un processus de double contrôle, puis validées par un analyste senior. Cette approche couvre l'ensemble du cycle de vie du risque tiers : découverte, priorisation, évaluation de maturité, analyse du risque et remédiation, avec un suivi continu et un reporting centralisé.

CyberVadis évalue des organisations dans plus de 110 pays, sur un modèle à coût mutualisé permettant un nombre illimité d'évaluations. L'entreprise est reconnue par l'ANSSI et membre de Hexatrust et de Campus Cyber.

À propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN rassemble plus de 1 300 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus : www.cesin.fr

Contact presse

CyberVadis : Marion Camurat · marketing@cybervadis.com · <https://cybervadis.com/fr>

CESIN : Véronique Loquet · 06.68.42.79.68 · <https://cesin.fr/>