SOURCE-TO-PAY

Une gestion des fournisseurs plus sûre grâce à l'automatisation intelligente

Comment les technologies d'IA réduisent les risques et préviennent la fraude fournisseurs

ESKER®

Dans cet e-book

La gestion des fournisseurs est une activité risquée

Mais l'automatisation pilotée par l'IA peut vous protéger contre toutes sortes de problèmes potentiels lors du processus d'intégration des fournisseurs.

Table des matières

De quelle fraude parle-t-on ? 3

Une nécessaire réduction des risques 4

Comment l'automatisation pilotée par l'IA prévient la fraude lors de l'intégration fournisseur 5

Questionnaires d'intégration générés par l'IA 6

Contrôles OFAC intégrés 8

Portails fournisseurs en libre service 9

Vérification automatique des coordonnées bancaires 10

Gestion centralisée des demandes fournisseurs 11

Agent Esker Synergy 12

Conclusion : pourquoi prendre le risque ? 14

À propos d'Esker 16

ESKER

Introduction

De quelle fraude parle-t-on ?

Qu’est-ce que la fraude fournisseur ?

De manière générale, on parle de fraude fournisseur lorsqu’un fournisseur trompe une entreprise afin qu’elle lui verse de l’argent en utilisant des tactiques telles que :

- **Surfacturation / manipulation des prix :** facturation supérieure au montant convenu ou montants des factures pour des biens ou des services gonflés ;
- **Facturation fictive :** envoi de factures pour des biens ou des services qui n’ont jamais été fournis ;
- **Faux fournisseurs :** création de sociétés écrans ou de faux comptes pour obtenir un paiement ;
- **Pots-de-vin / corruption :** cadeaux et incitations aux employés pour obtenir un traitement préférentiel ou approuver des paiements frauduleux ;
- **Substitution de biens / services :** livraison d’articles de qualité inférieure à celle spécifiée tout en effectuant la facturation pour des articles haut de gamme ;
- **Fraude à la facture :** usurpation de l’identité d’un véritable fournisseur par e-mail afin d’inciter les employés à effectuer des virements d’argent sur le compte d’un fraudeur.

Le risque croissant de fraude chez les fournisseurs

Malheureusement, la fraude des fournisseurs n’est pas près de disparaître. En fait, les conditions actuelles facilitent plus que jamais la tâche des fraudeurs.

- Les perturbations de la chaîne d’approvisionnement, telles que les droits de douane et les pénuries, obligent les entreprises à référencer rapidement de nouveaux fournisseurs, ce qui les conduit souvent à négliger certaines vérifications préalables.
- Des outils avancés comme l’IA générative aident les fraudeurs à se faire passer pour des fournisseurs et à modifier des factures, tandis que l’ingénierie sociale permet de tromper les employés.
- Des contrôles internes faibles, tels que des processus manuels, l’absence de séparation des tâches, une vérification insuffisante des fournisseurs et une surveillance médiocre créent des vulnérabilités importantes.
- Les systèmes existants sont souvent incapables de faire face aux techniques de fraude modernes.
- Les équipes financières cloisonnées peuvent, sans le savoir, faciliter la fraude en raison d’une mauvaise visibilité entre départements et d’une surveillance laxiste.

Une nécessaire réduction des risques

Personne ne souhaite exposer son organisation aux dommages financiers et à l'atteinte à la réputation que peuvent entraîner les fraudes aux paiements. Et à mesure que les techniques de fraude deviennent plus sophistiquées, il est plus important que jamais de protéger votre entreprise.

Le coût de la fraude

La fraude des fournisseurs coûte cher. Sans mesures de protection solides mises en place lors du processus d'intégration du fournisseur, vous exposez votre entreprise à :

Pertes liées à la fraude

- Vol de fonds sur les comptes
- Vols de biens et de services
- Coûts liés aux refacturations

Impact sur les partenaires

- Fournisseurs exerçant leur activité ailleurs
- Fournisseurs affectés par des contrôles stricts
- Faux positifs dans la vérification des comptes

Frais administratifs

- Frais juridiques
- Assurance
- Temps de travail perdu par le personnel

79 %

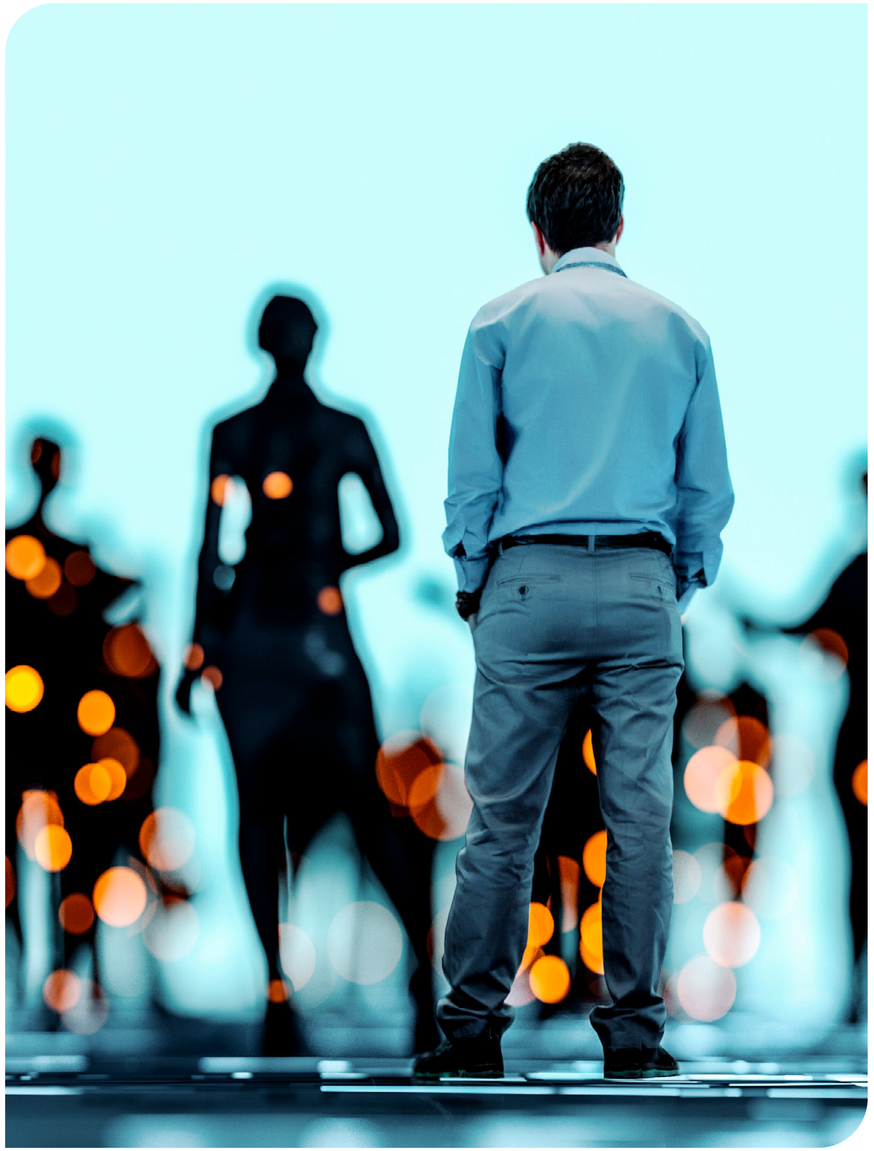
des organisations ont été victimes de fraudes aux paiements en 2024 [1]

362 milliards d'€

montant prévu des pertes dues à la fraude aux paiements d'ici 2028 [2]

7,7 %

de revenu annuel moyen perdu en raison de la fraude en 2025 dans le monde [3]



Comment l'automatisation pilotée par l'IA prévient la fraude lors de l'intégration fournisseurs

Espérer que votre entreprise puisse éviter des tentatives de fraude fournisseurs toujours plus sophistiquées en s'appuyant sur des outils traditionnels de gestion des fournisseurs revient à combattre un dragon avec un bouclier en carton. Face à une menace sérieuse, il faut des défenses solides. Les solutions d'automatisation pilotées par l'IA, conçues pour l'intégration et la gestion continue des fournisseurs, agissent comme de véritables remparts, protégeant votre organisation contre les attaques.

Une plateforme centralisée regroupant l'ensemble des données et des workflows liés aux fournisseurs permet à vos équipes d'évaluer et de surveiller plus efficacement les risques de fraude, tout en garantissant la conformité avec les contrôles internes et réglementaires. Le tout sans compromettre la qualité des relations avec vos fournisseurs stratégiques.

Mais concrètement, comment ça marche ? Voici six façons dont la plateforme d'automatisation pilotée par l'IA d'Esker vous protège contre la fraude à chaque étape du processus d'intégration fournisseurs :

- Questionnaires générés par l'IA
- Portail fournisseur en libre-service
- Contrôles OFAC intégrés
- Vérification automatique des coordonnées bancaires
- Gestion centralisée des demandes fournisseurs
- Agent Esker Synergy

Questionnaires d'intégration générés par l'IA

Le questionnaire d'intégration est un outil essentiel pour collecter des données auprès des fournisseurs potentiels afin d'évaluer leur légitimité, leurs capacités, leur conformité (sécurité, juridique, financière) et leur profil de risque avant leur validation en tant que fournisseur approuvé.

La création de ces questionnaires demande de l'expertise et du temps afin de s'assurer que toutes les bonnes questions sont posées, en fonction des régions et des secteurs d'activité dans lesquels vous et vos fournisseurs évoluez. Mais créer manuellement un nouveau questionnaire à chaque intégration fournisseur peut rapidement devenir un goulot d'étranglement.

C'est là que l'IA intervient. Grâce à un GPT *(Generative Pre-trained Transformer)* — un type de modèle de langage de grande taille (LLM, *Large Langage Model*) — il est possible de générer en quelques secondes des questions adaptées au secteur, à la zone géographique et au type de fournisseur concerné.

Comment ça fonctionne ?

Tout comme avec ChatGPT, il suffit de fournir au modèle GPT les exigences nécessaires, telles que les critères de conformité, les certifications attendues, les facteurs de risque, le nombre de questions souhaité ou encore le type de réponses (oui/non ou questions ouvertes, par exemple). **En quelques instants, le GPT génère un questionnaire complet et facilement modifiable de vérifications préalables couvrant tous les éléments indiqués dans la requête.**

L'IA peut adapter les questionnaires pour chaque fournisseur en fonction de sa localisation, de son secteur d'activité et des signaux de risque identifiés, de sorte que seules les informations pertinentes sont demandées. Cela permet non seulement d'améliorer la qualité des données collectées, mais aussi d'éviter aux fournisseurs de fournir des informations inutiles.

En résumé, l'IA aide vos équipes à collecter et analyser les informations plus efficacement dès cette étape clé du processus de l'intégration fournisseurs.

Les avantages des questionnaires d'intégration générés par l'IA

Gain de temps et de ressources : La réduction des tâches manuelles liées à la création des questionnaires permet à vos équipes de se concentrer sur des activités à plus forte valeur ajoutée, comme l'évaluation des risques et la gestion des relations fournisseurs.

Cohérence assurée : L'IA génère des questionnaires standardisés couvrant les critères essentiels de vérification préalable pour tous les fournisseurs, ce qui réduit les écarts et assure l'uniformité des données collectées.

Conformité renforcée : Vous évitez d'oublier des questions critiques liées à la conformité et restez en conformité avec les exigences réglementaires propres à chaque région et secteur d'activité.

Évolutivité : l'IA crée des questionnaires génériques qui peuvent être utilisés pour plusieurs fournisseurs, ce qui simplifie l'intégration des fournisseurs de tailles et de secteurs différents.

Facilité d'utilisation : Tous les membres de l'équipe peuvent créer un questionnaire, même sans expertise particulière, car l'IA guide le processus tout en garantissant la qualité.

Meilleure expérience fournisseur : La création plus rapide des questionnaires accélère l'intégration tout en garantissant que chaque fournisseur est évalué selon son profil de risque spécifique.

Portail fournisseurs en libre-service

Un portail fournisseur en libre-service rationalise le processus d'intégration des fournisseurs en offrant une interface sécurisée et intuitive pour soumettre leurs informations, documents, certifications et les autres éléments requis. La transmission d'informations via un portail élimine les échanges manuels d'information et accélère le processus de validation des fournisseurs.

Les portails améliorent l'efficacité, la transparence et la collaboration tout au long de l'intégration des fournisseurs — et au-delà — avec de nombreux bénéfices :

Gestion simplifiée des profils fournisseurs

Les fournisseurs peuvent mettre à jour les informations de leur profil, notamment leurs coordonnées, leurs informations bancaires et leurs certifications. En leur donnant la possibilité de gérer eux-mêmes leurs données, vous bénéficiez d'informations à jour et fiables, même après la phase initiale d'intégration.

Gestion documentaire facilitée

Le portail centralise et gère les documents fournisseurs pertinents, tels que les contrats, attestations d'assurance et documents de conformité. La collecte électronique de documents via un portail fournisseurs facilite leur partage et leur consultation, garantissant un accès rapide à l'information et réduisant les risques d'erreurs critiques.

Gestion des factures optimisée

Les portails ne se limitent pas à l'intégration. Les fournisseurs peuvent soumettre des factures électroniques, consulter et suivre leurs factures, et même vérifier le statut des paiements.
La transmission numérique des factures via un portail favorise la transparence, réduit les traitements manuels et améliore l'efficacité du processus Source-to-Pay (S2P), souvent chronophage.

Communication améliorée

Le portail établit un canal de communication efficace et transparent entre les partenaires commerciaux, permettant à votre organisation et à vos fournisseurs d'échanger des messages, de soumettre des demandes, de recevoir des mises à jour et de collaborer à la résolution des problèmes, dans un environnement numérique sécurisé.

32 %

des organisations utilisent actuellement un portail fournisseurs

43 %

des organisations déclarent qu'elles prévoient d'implémenter un portail fournisseur en libre-service dans les 1 à 2 prochaines années [4]

Contrôles OFAC intégrés

La vérification des fournisseurs au regard des listes de sanctions visant des entreprises, des personnes physiques ou des entités constitue une étape essentielle du processus de gestion des fournisseurs. Les sanctions sont généralement imposées par les gouvernements et les organismes internationaux, tels que les Nations unies (ONU), afin d'atteindre des objectifs de politique étrangère, de lutter contre le terrorisme, de prévenir le blanchiment d'argent ou de répondre à des préoccupations en matière de droits humains.

L'*Office of Foreign Assets Control* (OFAC), une division du département du Trésor américain, joue un rôle important à l'échelle mondiale dans l'application des sanctions économiques et commerciales. Cependant, il existe des dizaines de listes que les entreprises doivent consulter pour vérifier si des entités font l'objet de sanctions.

S'engager, même involontairement, dans des transactions avec une entité sanctionnée peut entraîner des violations réglementaires, de lourds dommages réputationnels et une perte de confiance de la part des partenaires et clients stratégiques.

Effectuer un paiement à une entreprise ou à une personne figurant sur une liste de sanctions peut créer de graves difficultés pour une organisation : problèmes juridiques, pertes financières, atteinte à la réputation, perturbation des processus métier, perte d'activité, renforcement du contrôle réglementaire…

Les défis du filtrage manuel des sanctions

De nombreux services de factures fournisseurs (AP) effectuent encore des contrôles manuels des entités au regard des listes de surveillance. Bien que le filtrage manuel puisse être efficace, il n'est pas infaillible et peut entraîner des problèmes importants :

- Des processus lents et chronophages
- Un risque accru d'erreurs
- Une couverture limitée
- Des faux positifs ou faux négatifs
- Un manque de scalabilité
- Une absence de traçabilité.

Les avantages du contrôle des sanctions intégré

Filtrage en temps réel

Le portail fournisseurs d'Esker permet de vérifier en temps réel les entreprises et les personnes physiques par rapport à des dizaines de listes de surveillance. Lorsque les fournisseurs saisissent leurs informations sur le portail, Esker compare leurs données aux listes les plus récentes et les plus complètes, notamment celles tenues à jour par des autorités telles que l'OFAC, l'Union européenne et l'ONU. Les acheteurs sont immédiatement informés en cas de correspondance potentielle avec une entité sanctionnée.

Couverture complète

Le contrôle des sanctions intégré au portail fournisseurs d'Esker offre une large couverture des listes de surveillance garantissant que toutes les listes pertinentes sont prises en compte lors des vérifications.

Efficacité et évolutivité accrues

Le filtrage automatisé des sanctions permet de traiter et d'analyser rapidement de grands volumes d'informations fournisseurs par rapport aux listes de surveillance. Les entreprises en forte croissance ou celles qui gèrent un grand nombre de fournisseurs n'ont pas besoin d'augmenter leurs effectifs pour suivre le rythme.

Conformité renforcée

Le contrôle des sanctions intégré au portail fournisseurs d'Esker documente le processus de vérification ainsi que ses résultats, fournissant une piste d'audit complète. Vous pouvez également accéder instantanément à des rapports sur les résultats des contrôles, les entités signalées et les actions engagées.

Intégration fluide avec les systèmes existants

Le portail fournisseurs d'Esker s'intègre de manière transparente à vos systèmes existants, comme les ERP, ce qui permet de mettre en place un processus fluide et automatisé tout au long du cycle de gestion des fournisseurs.

Vérification automatique des coordonnées bancaires

La vérification des comptes bancaires *(BAV, ou Bank Account Verification)* est un contrôle essentiel pour protéger les organisations contre tout accès non autorisé à leurs fonds, éviter les erreurs de paiement, les fraudes coûteuses, améliorer les relations commerciales et la sécurité financière globale. La vérification manuelle des comptes bancaires augmente le risque d'erreurs et laisse davantage de possibilités à des acteurs malveillants de passer entre les mailles du filet.

- Un numéro de compte bancaire peut être invalide
- Un compte bancaire peut ne pas appartenir au fournisseur concerné
- Un compte bancaire peut appartenir à un acteur malveillant
- Un compte bancaire peut être clôturé.

> **53 % des organisations s'appuient sur la validation verbale des coordonnées bancaires** [5]

La vérification des comptes bancaires est donc essentielle pour réduire le risque de paiements incorrects. Une solution automatisée de gestion des fournisseurs comme celle d'Esker permet d'éliminer les limites des contrôles manuels et de renforcer votre sécurité :

Prévention de la fraude

La vérification de la propriété des comptes bancaires aide les organisations à éviter les activités frauduleuses telles que l'usurpation d'identité et l'accès non autorisé aux fonds. En confirmant l'authenticité des informations bancaires et l'identité du titulaire du compte, les entreprises réduisent les risques de pertes financières et protègent leurs actifs.

Sécurité des paiements

Lorsque les entreprises effectuent des transactions financières, telles que des paiements à des fournisseurs (ou la réception de fonds de la part de clients), la vérification des comptes bancaires garantit que les fonds sont transférés aux bons réceptionnaires. Cela permet d'éviter les erreurs de paiement, les virements vers des comptes incorrects et les éventuels litiges financiers.

Conformité aux réglementations

De nombreuses juridictions ont mis en place des réglementations strictes pour lutter contre le blanchiment d'argent et le financement du terrorisme. Les entreprises doivent vérifier la titularité des comptes bancaires afin de respecter ces obligations et d'éviter tout paiement à des organisations ou individus faisant l'objet de sanctions gouvernementales. Le non-respect de ces exigences peut entraîner des conséquences juridiques et des atteintes à la réputation.

Renforcement de la confiance avec les partenaires et les fournisseurs

La mise en place d'un programme de vérification renforce la crédibilité et la fiabilité d'une organisation. L'automatisation de la vérification des comptes bancaires montre que votre organisation prend les mesures appropriées pour garantir la sécurité des transactions financières et protéger les intérêts de toutes les parties prenantes.

Gestion centralisée des demandes fournisseurs

Même si vous disposez d'une boîte e-mail dédiée à toutes les communications avec les fournisseurs, trier les messages pour identifier lesquels correspondent à des questions, des factures, des demandes de statut, des relances de paiement ou des mises à jour de profils fournisseurs peut rapidement devenir un travail à plein temps. De plus, toutes ces informations restent dispersées dans des e-mails individuels, ce qui complique l'obtention d'une vue complète de l'historique des échanges avec un fournisseur donné.

La solution *Esker Supplier Inquiry Management,* pilotée par l'IA, centralise toutes ces demandes fournisseurs (y compris les mises à jour importantes des coordonnées bancaires, des informations de contact ou des certifications) dans un tableau de bord unique et intuitif.

La solution identifie et catégorise automatiquement toutes les demandes entrantes selon leur type, afin de les orienter vers le workflow approprié pour traitement ou réponse. Pour les demandes nécessitant une réponse, Esker vous aide : l'IA analyse l'e-mail afin de comprendre la requête.

Si nécessaire, elle recherche ensuite les informations pertinentes dans les données internes de votre entreprise et génère un projet de réponse, que vos équipes peuvent relire afin d'en vérifier l'exactitude, la pertinence et y ajouter une touche de personnalisation.

Les fraudeurs tentent souvent de manipuler les données des fournisseurs, en particulier les changements de coordonnées bancaires ou les mises à jour d'information de contact. En centralisant toutes les demandes des fournisseurs dans un hub unique alimenté par l'IA, Esker est un outil précieux pour aider les entreprises.

Détectez les demandes de modification suspectes : chaque demande client est enregistrée, suivie et visible par les équipes Comptabilité fournisseurs et Achats en un seul endroit.

Réduisez le risque de phishing ou d'ingénierie sociale, car la plateforme évite les workflows dispersés par e-mail où les demandes frauduleuses passent souvent inaperçues.

Assurez une validation cohérente en plusieurs étapes : l'IA catégorise les demandes et peut inciter les équipes à appliquer les contrôles appropriés (comme une confirmation secondaire auprès du fournisseur).

Repérez les anomalies et les schémas suspects, tels que des délais inhabituels ou des tentatives répétées de mise à jour des coordonnées bancaires.

Esker Synergy Agent

Même si toutes vos informations liées au Sourcing, aux achats et à la comptabilité fournisseurs sont numérisées, retrouver rapidement une information précise peut encore sembler complexe — voire comparable à chercher une aiguille dans une botte de foin. L'agent Esker Synergy facilite la recherche, l'organisation et l'analyse de vos données fournisseurs. Besoin d'une liste de fournisseurs, d'un statut ou d'un rapport sur des indicateurs ? Il suffit de demander.

Posez des questions

comme "Quels fournisseurs présentent des indicateurs d'alerte dans notre système ?" et obtenez des réponses précises en temps réel. Cela vous permet de repérer les risques potentiels avant qu'ils ne s'aggravent.

Utilisez la fonction de reconnaissance vocale

pour récupérer rapidement les données de performance des fournisseurs ou les indicateurs de risque, même en déplacement, afin que vos équipes restent proactives et agiles.

Créez et enregistrez des vues personnalisées

avec des filtres dédiés aux fournisseurs à haut risque, aux retards de livraison ou aux signes d'instabilité financière.

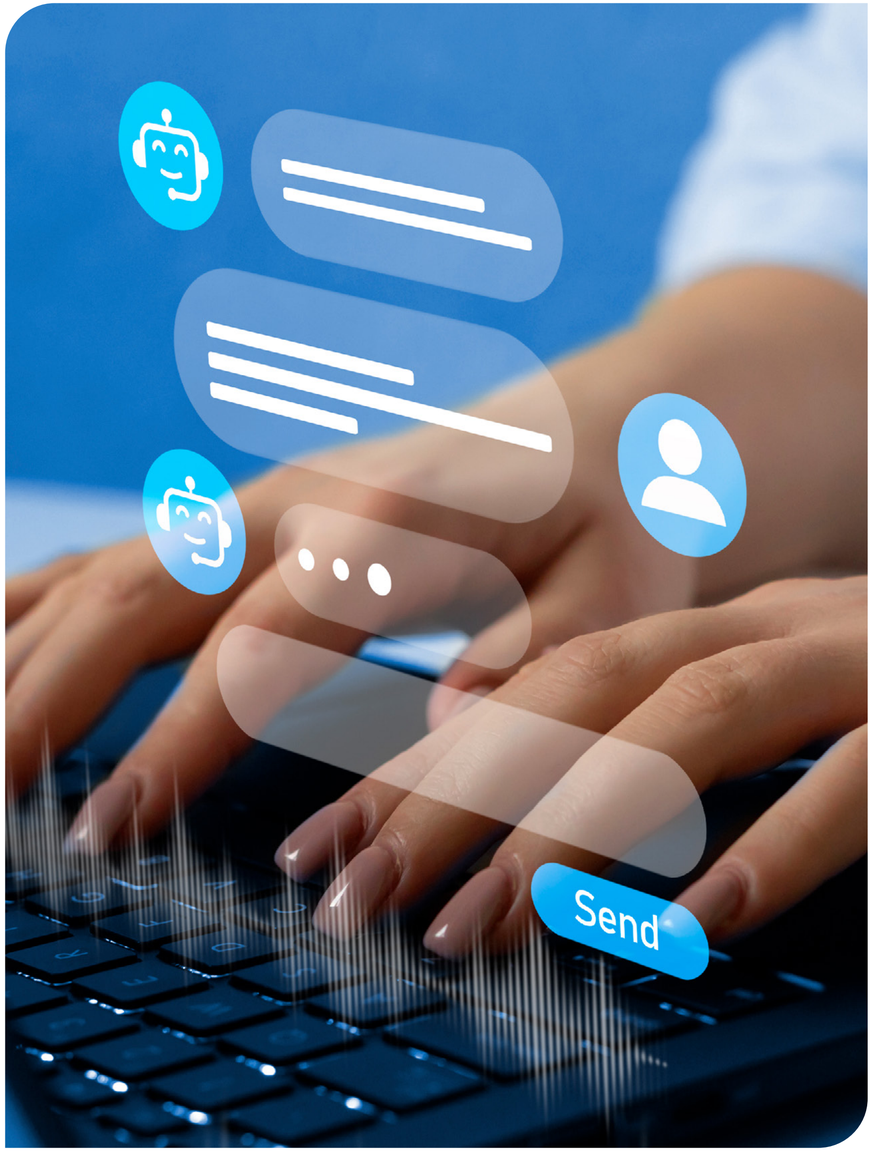
Posez des questions pratiques

et recevez des liens directs vers la documentation pertinente, ce qui vous aidera à maintenir la conformité et à réduire les risques sans passer des heures à chercher l'information.

Accédez en temps réel aux informations dont vous avez besoin pour accélérer la prise de décision tout en réduisant la charge administrative. Plus important encore, l'agent Esker Synergy vous aide à détecter les anomalies et les risques potentiels de fraude — par exemple des modifications inhabituelles des données fournisseurs ou des activités suspectes. Il permet ainsi des investigations plus rapides et des contrôles renforcés tout au long du cycle de gestion des fournisseurs.

L'agent Esker Synergy renforce la détection des fraudes en :

- **Identifiant rapidement les anomalies :** l'agent identifie les fournisseurs ayant récemment modifié leurs coordonnées bancaires, présentant des conditions de paiement inhabituelles ou des vérifications en retard, ce qui facilite la détection d'activités potentiellement frauduleuses.
- **Amélioration de la transparence :** Un accès instantané aux indicateurs fournisseurs, aux mises à jour de statut et à l'historique des activités permet aux équipes Achats et Comptabilité fournisseurs (AP) d'identifier des comportements irréguliers avant qu'ils ne s'aggravent.
- **Réduction des erreurs humaines :** en automatisant la récupération des données et la génération de rapports, l'agent minimise le risque d'oubli, un facteur courant dans les cas de fraude fournisseurs.
- **Accélération des mesures d'investigation :** Lorsqu'une activité suspecte est détectée, les équipes peuvent immédiatement interroger les données associées (par exemple les modifications concernant plusieurs fournisseurs) sans avoir à parcourir des feuilles de calcul ou des e-mails.



Conclusion

Pourquoi prendre le risque ?

Protégez votre entreprise contre la fraude en intégrant l'automatisation pilotée par l'IA dans la gestion des fournisseurs – et au-delà.

Alors que les risques augmentent et que les fraudeurs deviennent chaque jour plus sophistiqués et ingénieux, ce n'est plus le moment de rester passif en espérant que votre entreprise fera partie des rares à échapper aux pertes financières ou aux atteintes à la réputation. Les équipes financières qui souhaitent rester sécurisées, conformes et compétitives dans un monde en mutation adoptent dès aujourd'hui des solutions pilotées par l'IA afin de ne pas avoir à rattraper leur retard plus tard.

Si de nombreuses solutions permettent d'intégrer l'IA et l'automatisation à certaines étapes du processus de gestion des fournisseurs, Esker propose une plateforme unique d'automatisation pilotée par l'IA couvrant l'ensemble des cycles S2P (Source-to-Pay) et O2C (Order-to-Cash). Vous pouvez ainsi faire bénéficier toutes les équipes de l'*Office of the CFO* - la Direction financière étendue - des avantages de l'IA.

Mettre en œuvre une solution complète comme celle d'Esker vous permet de bénéficier de garde-fous technologiques qui sécurisent les paiements tout en simplifiant les tâches administratives, en améliorant la visibilité sur l'ensemble des processus S2P, en optimisant la communication interne et externe et en renforçant les relations avec les fournisseurs.

Sources

[1]2025 AFP® Payments Fraud and Control Survey Report, 2025, Association for Financial Professionals
[2]Combatting Online Payment Fraud, June 2023, Juniper Research
[3]H2 2025 Update to the Top Fraud Trends Report, October 2025, TransUnion
[4]Ardent Partners' Accounts Payable Metrics that Matter in 2023, 2023, Ardent Partners
[5]The Business Payments Coalition: A B2B Invoicing Standard, 2023, IOFM

Qui sommes-nous ?

La suite d'automatisation IA d'Esker pour l'*Office of the CFO* exploite les dernières technologies d'IA agentique et d'automatisation afin d'optimiser le fonds de roulement et la trésorerie, d'améliorer la prise de décision stratégique et de renforcer les relations humaines avec les clients, les fournisseurs et les équipes.

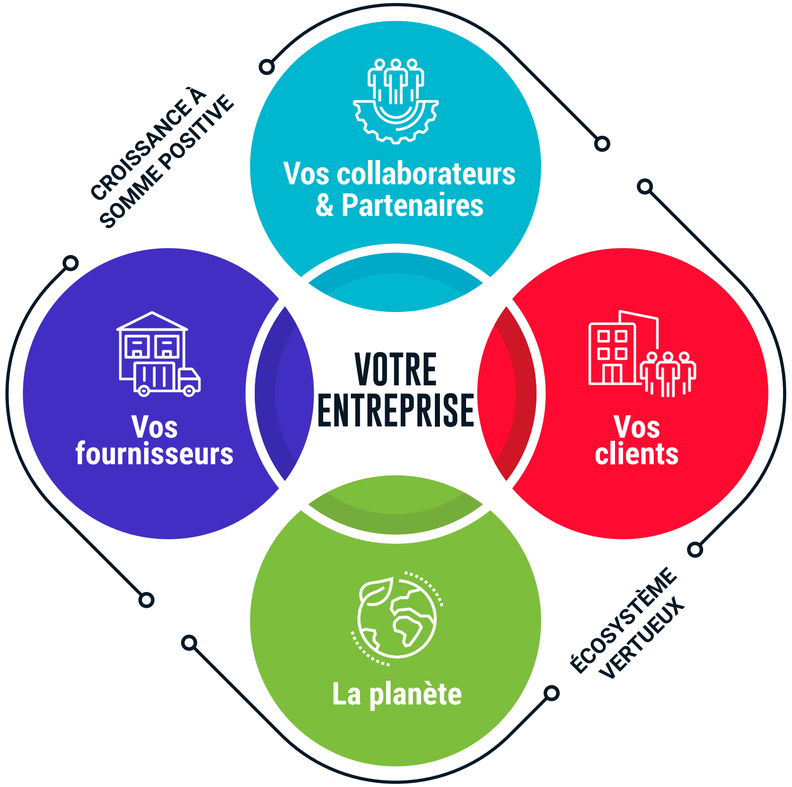
Les solutions Source-to-Pay et Order-to-Cash d'Esker automatisent tous les processus métier tout en soutenant les stratégies de croissance à long terme.

+ 40
années d'expérience dont plus de 20 ans dans le Cloud

+ 1 200
employé·e·s au service de plus de 1,12 million d'utilisateurs et de plus de 3 000 clients dans le monde

15
bureaux dans le monde, avec des sièges sociaux à Lyon (France) et Madison (États-Unis)

~250
millions d'euros de chiffre d'affaires en 2025



Construisons une croissance durable

Chez Esker, nous pensons que la seule façon de créer un changement réel et significatif est de viser une croissance à somme positive. Cela signifie atteindre le succès sans que cela se fasse au détriment d'un individu, d'un service ou d'une entreprise — tout le monde y gagne ! C'est pourquoi notre technologie pilotée par l'IA est conçue pour donner du pouvoir à chaque partie prenante tout en favorisant la création de valeur à long terme.

ESKER

ESKER®

www.esker.fr

© 2026 Esker S.A. Tous droits réservés. Esker et le logo Esker sont des marques commerciales ou des marques déposées d'Esker S.A. Toutes les autres marques sont la propriété de leur détenteur respectif.

016-FR-EBOOK-S2P-B