aprovall

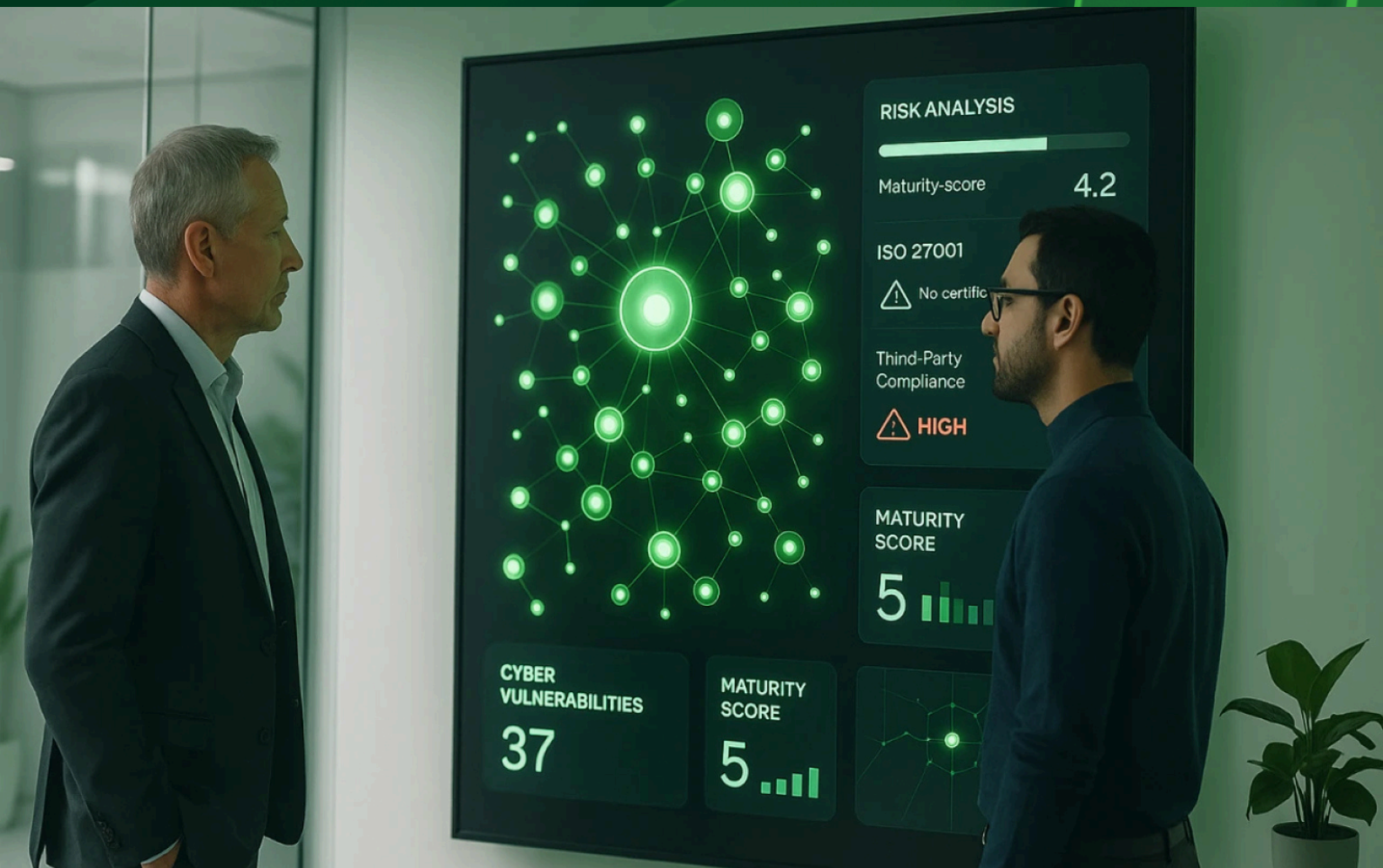
SisID An eftsure company

Trustpair

MARS 2026

Fraude aux coordonnées bancaires fournisseurs

Un défi majeur du TPRM



SOMMAIRE

PARTIE 1.

Anticiper et surveiller la fraude aux coordonnées bancaires fournisseurs : un enjeu clé du TPRM.

Trustpair : éliminer la fraude au virement en automatisant le contrôle de vos tiers

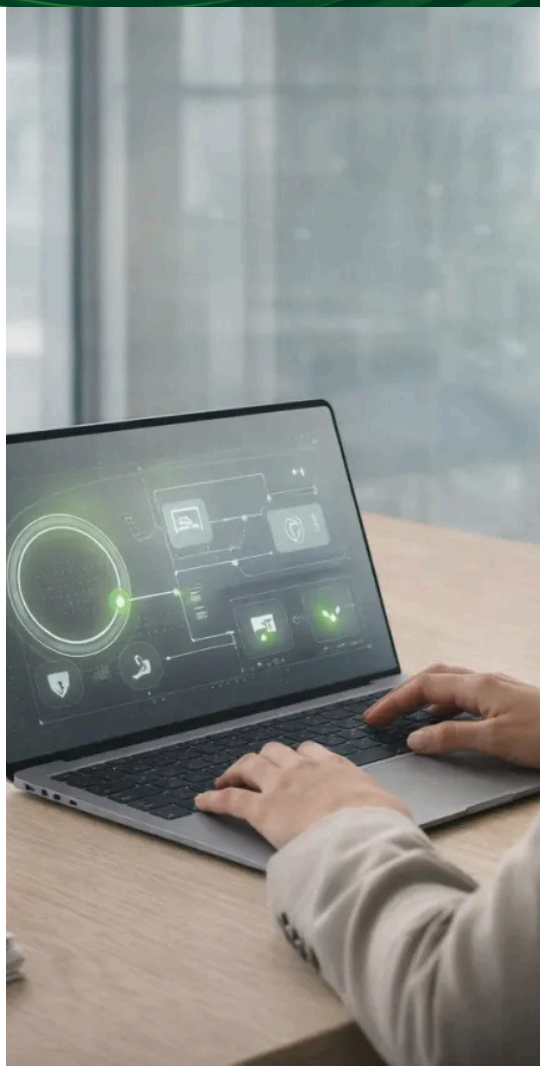
PARTIE 1.

Anticiper et surveiller la fraude aux coordonnées bancaires fournisseurs : un enjeu clé du TPRM

La fraude aux coordonnées bancaires fournisseurs connaît une croissance rapide et durable, au point de devenir l'un des risques financiers les plus critiques pour les organisations. Longtemps perçue comme marginale ou opportuniste, elle s'est transformée en une fraude structurée, industrialisée et répétitive, exploitant avant tout les failles organisationnelles plutôt que les vulnérabilités techniques.

Dans ce contexte, **sécuriser les coordonnées bancaires fournisseurs n'est plus une simple bonne pratique**, mais un impératif stratégique pour protéger les paiements, préserver la continuité d'activité et renforcer la gouvernance du risque tiers.

La digitalisation des échanges, l'extension des écosystèmes fournisseurs et la pression accrue sur les délais de paiement ont profondément modifié les conditions dans lesquelles opèrent les directions Finance, Achats et Conformité. Ces fonctions se trouvent aujourd'hui en première ligne face à un risque qui combine pertes financières directes, impacts juridiques, atteinte à la réputation et dégradation de la relation fournisseurs. C'est précisément dans ce contexte que les solutions de **Third Party Risk Management** (TPRM), telles qu'Aprovall, prennent toute leur dimension.



Une fraude en forte accélération, devenue systémique

La fraude aux coordonnées bancaires fournisseurs constitue désormais l'un des principaux vecteurs de pertes financières liées aux tiers. Elle touche indistinctement les grandes entreprises, les ETI, les PME et les organisations publiques, quels que soient leur secteur d'activité ou leur niveau de maturité technologique.

Les fraudeurs exploitent des failles communes : processus manuels, contrôles insuffisamment formalisés, dépendance aux échanges par email et absence de vérification indépendante lors des changements de coordonnées bancaires.

Les chiffres illustrent clairement l'ampleur du phénomène. Plus de la moitié des fraudes bancaires constatées aujourd'hui sont liées à des scénarios de faux fournisseurs ou de modifications frauduleuses de RIB, avec un **montant moyen par fraude avoisinant 70 000 euros**. Un faux RIB peut rester actif pendant plusieurs mois, générant des détournements successifs et touchant parfois simultanément plusieurs organisations. Cette capacité de propagation démontre que la fraude ne relève plus de cas isolés, mais bien d'un **risque systémique**, appelé à s'intensifier dans les prochaines années.

Dans ce contexte, la sécurisation des paiements fournisseurs ne peut plus être considérée comme une simple mesure de conformité ou un contrôle ponctuel. Elle devient un **enjeu de pérennité financière et de gouvernance globale du risque tiers**.

Typologies de fraude aux coordonnées bancaires fournisseurs

La fraude aux coordonnées bancaires, souvent désignée sous le terme de Vendor Payment Fraud, recouvre plusieurs scénarios distincts, qui sont dans la pratique fréquemment combinés. Le plus courant consiste pour un fraudeur à se faire passer pour un fournisseur légitime afin de solliciter un changement de coordonnées bancaires. Cette usurpation repose généralement sur l'exploitation d'informations publiques, de données compromises ou de communications interceptées, rendant la demande crédible et difficile à détecter.

D'autres scénarios incluent la modification frauduleuse de RIB ou d'IBAN lors de l'onboarding fournisseur ou à l'occasion d'une mise à jour administrative. Les attaques par compromission d'email (Business Email Compromise – BEC) permettent quant à elles d'imiter ou d'intercepter des échanges internes ou fournisseurs. Ces attaques sont souvent renforcées par des techniques d'ingénierie sociale exploitant l'urgence, la pression hiérarchique ou des périodes sensibles comme les clôtures comptables.

Dans certains cas plus complexes, la fraude peut également impliquer une collusion interne ou s'inscrire dans des schémas plus larges de fraude au président. Quel que soit le scénario, le point commun reste l'exploitation de failles organisationnelles et procédurales, bien plus que de vulnérabilités purement techniques.

À noter

Un fraudeur se fait passer pour un faux fournisseur et vous demande de modifier les coordonnées bancaires pour les prochains paiements

Origine et mécanismes des fraudes bancaires fournisseurs

Les fraudes aux coordonnées bancaires reposent rarement sur une cause unique. Elles résultent le plus souvent d'une combinaison de facteurs humains, organisationnels et contextuels. Les réseaux de cybercriminalité ont considérablement affiné leur connaissance des processus internes des entreprises, leur permettant de reproduire fidèlement les usages, le vocabulaire et les cycles de validation.

Le facteur humain joue un rôle central dans la réussite de ces attaques. La pression sur les délais de paiement, la surcharge opérationnelle des équipes finance ou comptabilité fournisseurs, ainsi que l'absence de contrôles systématiques réduisent la capacité à exercer une vigilance constante.

Le scénario le plus fréquemment observé reste celui du faux fournisseur : une demande de modification de coordonnées bancaires, formulée de manière crédible et contextualisée, est validée sans vérification indépendante. Le paiement est alors détourné, souvent sans détection immédiate, parfois sur plusieurs cycles de paiement.

Le facteur humain et organisationnel : principal point de vulnérabilité

Malgré les progrès des technologies de sécurité, la fraude aux coordonnées bancaires continue de prospérer en exploitant des processus encore largement manuels. Dans de nombreuses organisations, les échanges reposent toujours sur des emails, des fichiers Excel ou des formulaires PDF, avec des validations parfois informelles et une traçabilité limitée.

L'absence de ségrégation des tâches, le manque de double validation ou l'insuffisance de sensibilisation aux signaux faibles fragilisent considérablement les dispositifs de prévention. Lorsque le contrôle repose principalement sur la vigilance individuelle plutôt que sur des processus structurés et automatisés, le risque de fraude augmente mécaniquement.

Un impact financier largement sous-estimé

La fraude aux coordonnées bancaires est souvent appréhendée uniquement à travers le montant détourné. Or, son impact réel est bien plus large. Pour compenser une fraude, une entreprise doit générer un chiffre d'affaires équivalent à **environ six fois le montant perdu**, ce qui illustre le poids économique réel de ces incidents.

À cette perte directe s'ajoutent de nombreux coûts indirects : enquêtes internes, frais juridiques, délais de recouvrement incertains, mobilisation prolongée des équipes et perturbation des opérations. Les impacts réputationnels et la dégradation de la relation de confiance avec les fournisseurs peuvent également avoir des conséquences durables, parfois difficiles à quantifier.

Sur le plan réglementaire et juridique, ces incidents interrogent directement l'efficacité des dispositifs de contrôle interne et la gouvernance du risque, notamment lors d'audits internes ou externes.

Les zones de risque dans le cycle de vie fournisseur

La fraude aux coordonnées bancaires ne survient pas de manière aléatoire.
Elle se concentre sur des moments précis du cycle de vie fournisseur, en particulier lors de l'onboarding initial et lors des demandes de modification de coordonnées bancaires. Ces étapes sont souvent réalisées sous contrainte de délai, ce qui réduit le niveau de vigilance.

L'absence de traçabilité des contrôles, le manque d'indépendance dans les validations et l'utilisation de processus manuels non sécurisés constituent autant de points de vulnérabilité. C'est précisément à ces moments critiques que des contrôles systématiques, traçables et auditables doivent être intégrés de manière native.

Trustpair

PAROLE D'EXPERT

Trustpair : éliminer la fraude au virement en automatisant le contrôle de vos tiers

La fraude au virement : un risque sous-estimé, une menace qui explose

La fraude au virement est devenue l'un des premiers risques financiers auxquels font face les entreprises françaises. Et la tendance ne faiblit pas : en 2025, la fraude sur les moyens de paiement en France a atteint 618 millions d'euros au premier semestre seulement *(Observatoire de la sécurité des moyens de paiement, Banque de France)*.

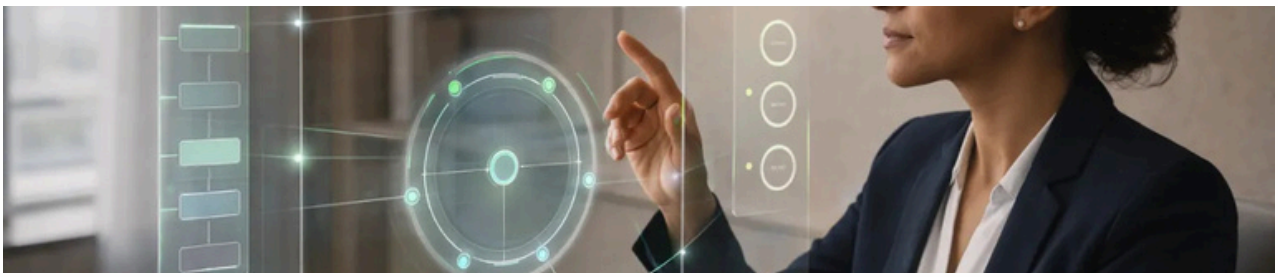
Pour les Directions Achats, l'exposition est directe : chaque création ou modification de coordonnées bancaires fournisseur est un point de vulnérabilité. La fraude au faux fournisseur, où un escroc usurpe l'identité d'un tiers pour détourner un virement, est aujourd'hui l'une des techniques les plus utilisées contre les entreprises.

Les fraudeurs ont muté. Les contrôles manuels, non.

Ce qui a changé en profondeur, c'est la sophistication des attaques. Boostés par l'IA générative, les fraudeurs produisent désormais des emails parfaits, des documents falsifiés indétectables et des deepfakes audio ou vidéo imitant la voix de vos dirigeants ou partenaires. 71 % des entreprises ont enregistré une hausse des tentatives de fraude assistées par l'IA (Rapport Trustpair 2026).

Face à cette réalité, les dispositifs de contrôle manuels traditionnels, rappels téléphoniques, vérifications par email, circuits de validation papier, ne tiennent plus la route :

- Ils sont lents et consomment des ressources précieuses dans vos équipes
- Ils reposent sur des données non vérifiées en temps réel
- Ils créent une fausse impression de sécurité : 58 % des entreprises estiment que les fraudeurs évoluent plus vite que leurs équipes ne peuvent répondre *(Rapport Trustpair 2026)*
- Ils exposent à l'erreur humaine, première cause de fraude réussie



La réponse : automatiser la vérification des coordonnées bancaires fournisseurs

La prévention de la fraude au virement ne peut plus reposer sur la vigilance humaine seule. Elle doit s'appuyer sur une vérification automatisée, systématique et en temps réel des RIB fournisseurs, à chaque création, modification, et avant chaque paiement.

C'est précisément ce que propose Trustpair : une plate-forme anti-fraude qui automatise le contrôle de la corrélation entre l'identité d'un tiers et ses coordonnées bancaires.

Avec Aprovall, le gain de temps a été immédiat.

La digitalisation du contrôle bancaire automatise les tâches et renforce la lutte contre la fraude bancaire. La solution permet aussi de vérifier tous nos tiers, directs et indirects, une mission autrement laborieuse.

Stéphanie Nicoud
Responsable Anti-mafia & Régularité des Fournisseurs TELT

Ce que cela change concrètement pour les Directions Achats :

Là où le contrôle manuel se limite à des vérifications ponctuelles et incomplètes, Trustpair assure un contrôle continu sur 100 % du panel fournisseurs. L'automatisation permet des contrôles jusqu'à 10 fois plus rapides, libérant vos équipes des tâches chronophages à faible valeur ajoutée pour qu'elles se concentrent sur l'essentiel. Et là où la sécurité dépend de la vigilance des équipes, Trustpair constitue un filet de sécurité systématique, indépendant de l'humain. Chaque contrôle est tracé, facilitant la conformité et les audits.

La plateforme couvre 190 pays, permettant aux entreprises ayant un panel fournisseurs international de bénéficier du même niveau de contrôle quel que soit le pays d'origine du fournisseur — un enjeu majeur pour les grandes entreprises et ETI opérant à l'international.

Enfin, Trustpair s'intègre nativement dans votre écosystème applicatif grâce à plus de 20 connecteurs natifs, dont une connexion directe avec Aprovall. Cela signifie que la vérification anti-fraude peut s'activer directement dans votre processus de gestion des tiers, sans rupture de flux ni ressaisie manuelle.

Pourtant, seules 32 % des entreprises valident en continu les données bancaires de leurs fournisseurs (Rapport Trustpair 2026). Les 68 % restants s'exposent à une fraude qui peut coûter des dizaines, voire des centaines de milliers d'euros par incident.

100%
des panel fournisseurs en contrôle continu

10x
plus rapide avec l'automatisation des contrôles

190
pays couverts par la plateforme

+20
connecteurs natifs

En résumé : la digitalisation n'est plus une option

Dans un environnement où les fraudes se multiplient et se sophistiquent, automatiser le contrôle des tiers est devenu une nécessité opérationnelle. Pour les Directeurs Achats, c'est aussi une question de responsabilité : la sécurisation des flux de paiement commence dès la gestion du référentiel fournisseurs.

Trustpair s'intègre directement dans vos systèmes (ERP, P2P, outil de gestion des tiers) pour faire de la vérification anti-fraude une composante invisible mais permanente de votre processus achats.

PARTIE 2.

Sécuriser les paiements fournisseurs grâce à une approche TPRM

Face à un risque devenu systémique, la réponse ne peut être fragmentée. La sécurisation des coordonnées bancaires doit s'inscrire dans une **approche globale de Third Party Risk Management**. Les données bancaires fournisseurs doivent être collectées via des canaux sécurisés, par des référents identifiés, puis vérifiées de manière indépendante avant toute activation.

Chaque contrôle doit être documenté, horodaté et conservé comme preuve de diligence. Cette approche permet de sécuriser les paiements sans alourdir inutilement les processus, tout en améliorant la qualité, la fiabilité et la gouvernance des données fournisseurs.

SisID An eftsure company

LYON PART-DIEU Société Publique Locale

Nous avons pu détecter et éviter une tentative de fraude de 1,7 M d'€

Grâce au contrôle des coordonnées bancaires via Sis ID & Aprovall, nous avons pu détecter et éviter une tentative de fraude de 1,7 million d'euros. Sans cette vérification en amont, la chaîne de paiement aurait pu être vulnérable. Ce type d'incident montre à quel point il est essentiel de s'appuyer sur des outils fiables afin de sécuriser nos processus.

Antoine Nourry
Responsable Administratif & Financier | SPL

Prévenir durablement la fraude : contrôles, technologies et culture

La prévention efficace de la fraude aux coordonnées bancaires repose sur un équilibre entre trois leviers complémentaires.

1. Le premier est **organisationnel** : double validation, ségrégation des tâches, gestion formalisée des exceptions et responsabilisation claire des acteurs.

2. Le deuxième est **technologique** : vérification automatisée des coordonnées bancaires, contrôles ex ante, journalisation des actions et intégration native aux ERP et SRM.

3. Le troisième est **culturel** : sensibilisation continue des équipes et formation à la détection des signaux faibles.

C’est la combinaison de ces leviers qui permet d’inscrire la prévention dans la durée.

Intégrer la vérification des coordonnées bancaires aux phases clés de la relation d'affaires

La sécurisation des coordonnées bancaires fournisseurs ne peut être efficace que si elle s'inscrit dans l'ensemble du **cycle de vie de la relation d'affaires**. Limiter les contrôles à un moment unique expose l'entreprise à des failles importantes. Une approche structurée doit couvrir quatre phases essentielles : **l'évaluation préalable, l'onboarding, le monitoring continu et l'offboarding**.

1

Évaluation préalable

Dès la phase d'évaluation préalable, la vérification des coordonnées bancaires permet d'identifier les incohérences potentielles entre l'identité juridique du tiers, sa domiciliation et les informations bancaires fournies. Cette étape contribue à filtrer les risques en amont et à orienter les décisions d'engagement.

2

Onboarding

Lors de l'onboarding, la création des coordonnées bancaires doit être strictement encadrée : collecte via des canaux sécurisés, vérification indépendante des RIB, validation par des acteurs distincts et traçabilité complète des contrôles. Cette phase est critique, car toute erreur ou fraude initiale peut être exploitée durablement.

3 Monitoring continu

Le monitoring continu est tout aussi essentiel. Les coordonnées bancaires ne sont pas figées : elles peuvent évoluer légitimement, mais chaque modification doit déclencher un nouveau cycle de vérification, assorti d'alertes et de contrôles renforcés.

4 Offboarding

Enfin, l'offboarding est trop souvent négligé. À l'arrêt de la relation d'affaires, la suppression ou la désactivation des coordonnées bancaires est indispensable pour éviter toute réutilisation frauduleuse ultérieure et garantir l'intégrité du référentiel fournisseurs.

Espacil Habitat
Groupe ActionLogement

Aprovall sécurise nos coordonnées bancaires et réduit le risque de fraude.

Le module SIS ID intégré dans Aprovall nous a permis de sécuriser complètement la création ou la modification des coordonnées bancaires. Le contrôle du couple SIRET–IBAN, avec le système de feux vert/orange/rouge, a fortement réduit les risques de fraude.

Flavie Tremaudan
Juriste référent Achats

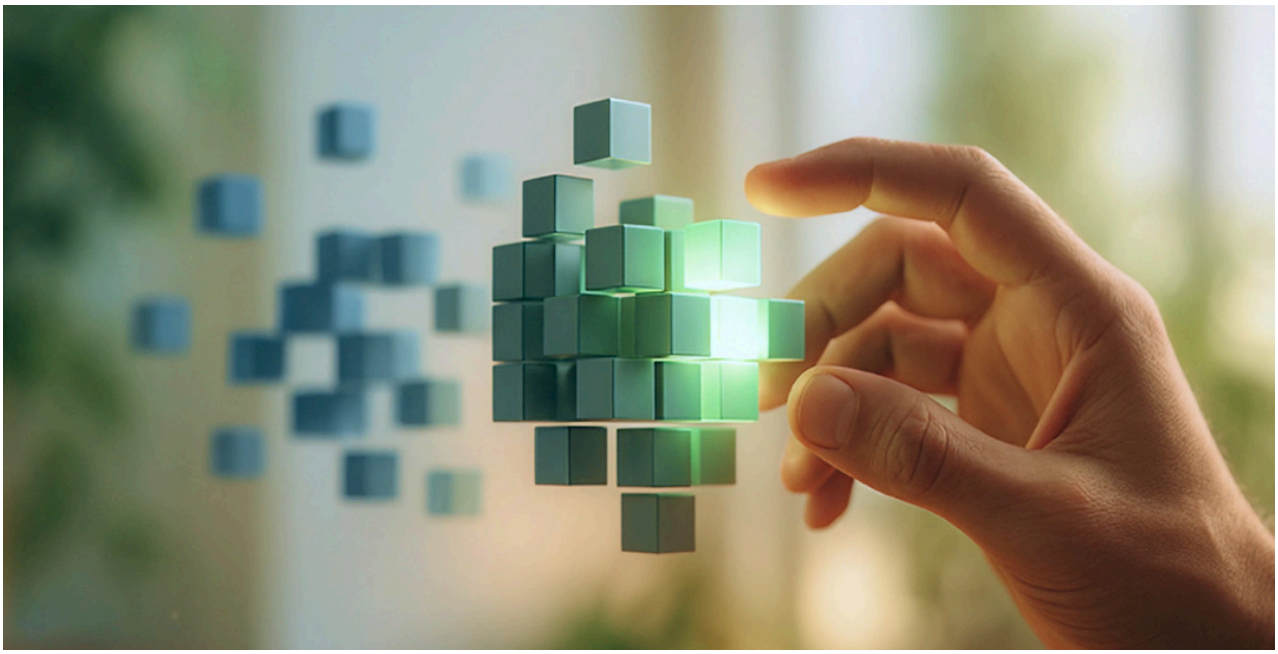
Une fausse impression de sécurité

L'automatisation des factures peut créer un sentiment de sécurité excessif. Une facture électronique conforme, transmise via une plateforme agréée, peut parfaitement contenir des coordonnées bancaires frauduleuses si celles-ci ont été modifiées en amont dans le référentiel fournisseur.

Le risque se déplace alors :

- non plus au moment de la réception de la facture,
- mais **au moment de la création ou de la modification des coordonnées bancaires du fournisseur.**

Autrement dit, une fraude réussie en amont est ensuite amplifiée par des processus automatisés en aval. La facturation électronique peut ainsi accélérer l'exécution du paiement frauduleux si les contrôles de modification de RIB ne sont pas robustes, indépendants et traçables.



Des vecteurs de fraude toujours actifs

La facturation électronique n'élimine pas les scénarios classiques de fraude aux coordonnées bancaires :

- Demandes de changement de RIB transmises par email en parallèle du circuit officiel,
- Usurpation d'identité d'un fournisseur légitime,
- Compromission de comptes utilisateurs internes ou fournisseurs,
- Exploitation des périodes de transition (déploiement de la réforme, coexistence des anciens et nouveaux processus).

Dans ces contextes, les fraudeurs adaptent leurs méthodes pour exploiter les zones grises organisationnelles, notamment lorsque les responsabilités entre facturation, référentiel fournisseur et paiement ne sont pas clairement définies.

PAROLE D'EXPERT

SIS ID

Usurpation d'identité, compromission de messageries, falsification de RIB lors d'un changement de coordonnées : les scénarios sont connus, mais les attaques restent efficaces car elles exploitent avant tout des failles humaines et organisationnelles. Là où les contrôles ne sont ni systématiques ni centralisés, la fraude s'insère discrètement dans le cycle de vie fournisseur.

Dans ce contexte, le Third-Party Risk Management doit évoluer : au-delà de l'évaluation des données tiers, il doit intégrer un contrôle opérationnel et continu de l'authenticité des données de paiement, dès l'onboarding et jusqu'au paiement.

Intégrer la vérification bancaire comme standard de gouvernance

La clé d'une automatisation des processus réellement sécurisée repose sur le caractère incontournable et systématique des contrôles d'authenticité des données traitées. C'est ici que la valeur de solutions de sécurisation intégrées au cœur du TPRM prend tout son sens. Entièrement intégré à la plateforme **Aprovall, Sis ID** vérifie la validité des coordonnées bancaires de vos tiers.

Chaque vérification fournit un statut clair :

- Compte correctement rattaché au bénéficiaire,
- Incohérence détectée,
- Risque potentiel de fraude.

Disponible dans plus de 200 pays et territoires, Sis ID renforce la capacité d'évaluation TPRM d'Aprovall en permettant de traiter le risque de fraude bancaire dès la première étape d'intégration des partenaires et jusqu'à l'exécution du paiement.

Au-delà de la vérification ponctuelle, l'enjeu est d'inscrire ce contrôle dans les zones critiques du cycle fournisseur :

1. **Onboarding** : validation des coordonnées à la création de la fiche tiers dans l'ERP.
2. **Modification de RIB** : contrôle automatique et incontournable lors de toute demande de changement.
3. **Contrôle régulier des tiers sensibles** : surveillance continue des comptes stratégiques.
4. **Avant paiement** : point de contrôle instantané avant chaque transaction.

À noter

La sécurisation grâce à l'automatisation, mais pas seulement

La lutte contre la fraude ne peut reposer uniquement sur des contrôles manuels, chronophages et hétérogènes. Mais l'automatisation seule ne suffit pas non plus.

Sis ID a été conçu pour combiner puissance technologique, interconnexion des bases de données et supervision experte. L'objectif est double : fluidifier les opérations et garantir leur sécurité.

L'automatisation des contrôles permet d'authentifier les données de manière fiable et fluide cependant lorsque des incohérences sont remontées, le risque persiste. Pour couvrir le besoin de contrôle supplémentaire, les équipes expertes Sis ID interviennent de manière ciblée pour couvrir les angles morts que l'automatisation peut laisser subsister.

L'intégration dans **Aprovall Manager** permet :

- d'insérer la vérification des données tiers directement dans les workflows de validation,
- de centraliser les résultats pour l'ensemble des équipes finance, achats et compliance,
- d'éviter les frictions et les contrôles redondants,
- de garantir une traçabilité complète à des fins d'audit.

La connexion des outils et des référentiels assure que chaque mise à jour bénéficie immédiatement à l'ensemble de l'organisation, tout en restant strictement protégée.

Anticiper plutôt que réparer : un impératif stratégique

L'impact financier de la fraude bancaire fournisseur est souvent sous-estimé. Au-delà de la perte directe, il faut intégrer le coût interne de gestion de crise, les audits correctifs, les tensions fournisseurs et l'atteinte à la réputation.

C'est pourquoi la sécurisation des coordonnées bancaires doit devenir un standard, et non une mesure corrective après incident.

Pensé pour accompagner les directions financières et les équipes TPRM à chaque étape du processus de paiement, Sis ID apporte sérénité et maîtrise du risque.

À ce jour, plus de 7 000 tentatives de fraude ont été détectées et stoppées pour nos clients. L'un des cas récents, celui de la SPL, illustre concrètement cette réalité : une tentative de modification frauduleuse identifiée en amont, un paiement bloqué avant exécution, et une exposition financière de 1,7 millions d'euros évitée

PARTIE 3.

Vers une gouvernance renforcée des paiements à l'ère de la dématérialisation

La montée en puissance de la facturation électronique rend plus que jamais nécessaire une gouvernance transverse des données fournisseurs, impliquant finance, achats, conformité et IT.

Les entreprises qui anticipent cette convergence entre dématérialisation et TPRM évitent l'écueil d'une automatisation aveugle et transforment la réforme en opportunité de renforcement du contrôle interne.

À noter

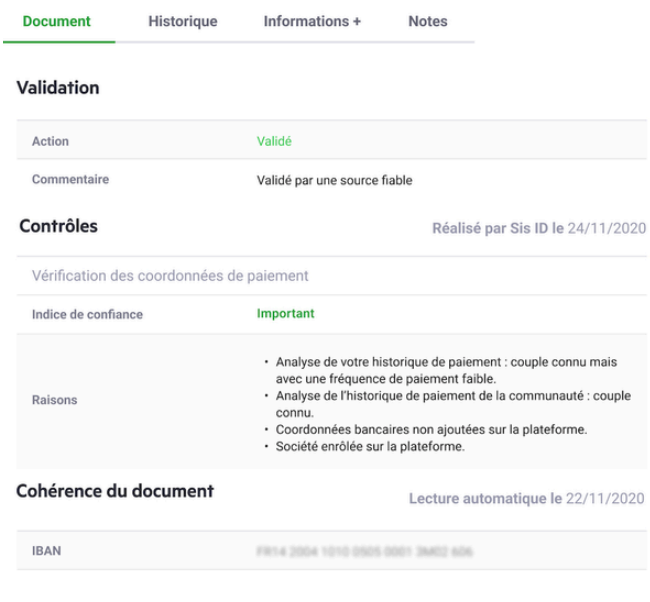
La facturation électronique sécurise le flux,
le TPRM sécurise la donnée.

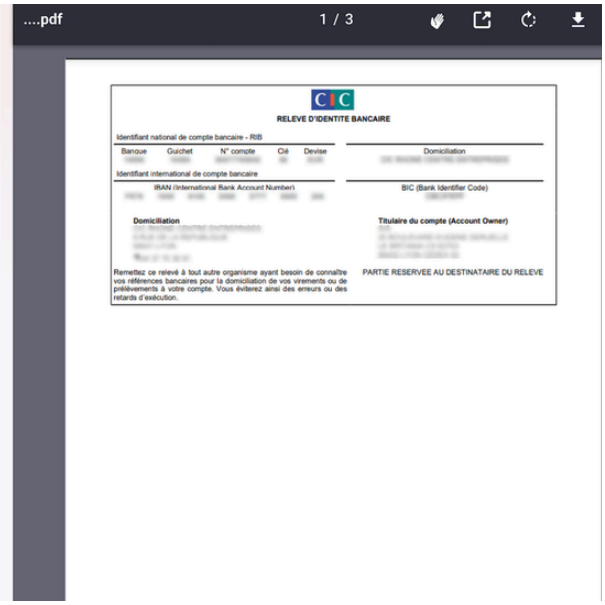
C'est la combinaison des deux qui permet de lutter efficacement et durablement contre la fraude aux coordonnées bancaires fournisseurs.

Intégrer la vérification bancaire au cœur du TPRM

La vérification des coordonnées bancaires fournisseurs ne doit jamais être envisagée comme un contrôle isolé. Elle doit intervenir dès l'entrée en relation fournisseur, lors de chaque modification et s'inscrire dans une logique de surveillance continue du risque tiers.

Intégrée au TPRM, elle devient un pilier de gouvernance, au même titre que les contrôles de conformité, de cybersécurité ou de continuité d'activité.

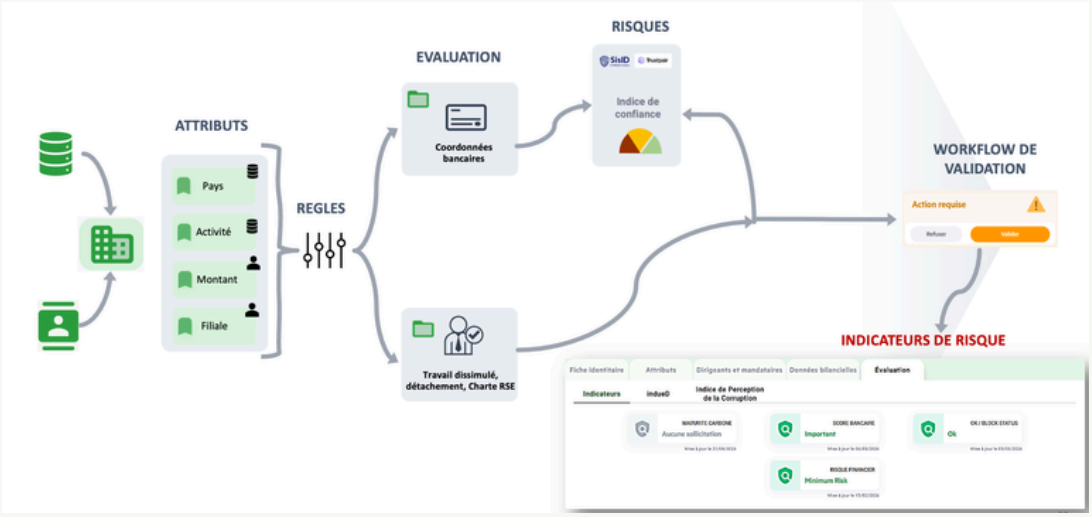




Des processus prêts à l'emploi avec Aprovall Manager

Aprovall Manager propose un parcours de bout en bout conçu pour répondre à ces enjeux. La solution permet une collecte sécurisée des coordonnées bancaires fournisseurs, une vérification automatisée et indépendante, ainsi que la génération de preuves de contrôle horodatées et auditables.

Grâce aux notifications en temps réel, aux workflows de validation et à l'intégration native aux outils métiers, les équipes sécurisent durablement les paiements tout en améliorant la fluidité des processus et la qualité des données fournisseurs.



L'objectif

Réduire drastiquement le risque de fraude aux coordonnées bancaires, tout en **renforçant** la gouvernance du risque tiers et la **sérénité** des opérations.

Aprovall

Aprovall, est un leader européen des logiciels de gouvernance, de gestion des risques et de conformité des tiers (TPGRC) .

Grâce à sa plateforme Aprovall Manager, ses clients bénéficient de l'ensemble des évaluations et des informations nécessaires tout le long du cycle de vie des relations avec leurs tiers, assurant leur conformité, la protection de leurs actifs et de leur réputation dans un environnement de plus en plus complexe et contraignant.

Pour en savoir plus, visitez www.aprovall.com

Nos engagements

SILVER | Top 15% ecovadis Sustainability Rating DEC 2025

SERVICE FRANCE GARANTI BV Cert. 18968694 relation client

GES 10,3kg/k€

ISO 27701 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification