Connaître les schémas de fraude

YAHIAOUI Mohamed
Commissaire aux Comptes

Diplômé en finances des Universités de Paris Sorbonne et Paris Dauphine.

Alger, le 21 juillet 2025.

الغرفة الوطنية لمحافظي الحسابات
CHAMBRE NATIONALE DES
CNCC
COMMISSAIRES AUX COMPTES

Pourquoi connaître les schémas de fraude ?

- La fraude ne se résume pas à des actes isolés : elle suit **des logiques, des séquences et des opportunités**.
- La détection repose sur la **capacité à reconnaître ces schémas** récurrents dans les organisations.
- Même si l'auditeur applique les **diligences normales**, la **dissimulation volontaire** des actes frauduleux rend leur repérage difficile.
- Avant de chercher à détecter, il faut **savoir ce que l'on cherche** : les schémas permettent de **structurer l'analyse du risque**.
- **Message clé :** Étudier les schémas, c'est poser les bases d'une détection efficace et d'un système de contrôle pertinent.

Caractéristiques communes des schémas de fraude

Des mécanismes simples, des variantes infinies

Principe de base : exploiter une faille (humaine, technique, organisationnelle)

- **Points d'appui fréquents** :
  - **Défaut de séparation des tâches**
  - **Absence de contrôle croisé**
  - **Manque de documentation ou de traçabilité**
- **Adaptation au contexte** :
  - Chaque schéma se moule dans l'organisation cible (secteur, culture, outils…)
  - Le **mode opératoire reste simple** : double facturation, fausse écriture, faux client…
- Ce n'est pas la complexité qui fait la fraude, mais **la négligence ou la confiance mal placée.**
- **Message clé :** Une bonne organisation empêche souvent des fraudes basiques mais récurrentes.

Les risques pour les dirigeants et les organisations

Pourquoi les chefs d'entreprise doivent s'impliquer

- La connaissance des schémas est un **outil stratégique de prévention** pour les décideurs.
- Une fraude, même simple :
  - **Coûte cher** (pertes financières directes et coûts juridiques)
  - **Ternit la réputation** (perte de confiance des partenaires et des clients)
  - **Expose les dirigeants** (responsabilité pénale, image publique)
- L'implication du management permet de :
  - **Ancrer une culture du contrôle**
  - **Former les équipes** à reconnaître les signaux faibles
  - **Soutenir les dispositifs d'alerte** (lanceurs d'alerte internes)
- **Message clé :** La lutte contre la fraude commence **au sommet**, par une culture éthique et des signaux clairs.

Transition – Vers une typologie par processus

Classer les schémas pour mieux les combattre

- Deux grandes **familles de schémas de fraude** :
  - **Schémas opérationnels**, au cœur des **processus métier** (achats, paie, ventes…)
  - **Schémas comptables et financiers**, visant les **états financiers** (résultats, bilans, provisions…)
- Chaque processus peut comporter ses propres **zones de vulnérabilité**.
- Cette typologie servira de **grille de lecture** pour analyser les cas concrets et renforcer les contrôles internes.
- **Message clé :** Décomposer les fraudes par processus permet une **cartographie ciblée du risque** et une réponse adaptée.

Les limites de l'identification des schémas

Pourquoi l'approche par typologie reste imparfaite ?

- **Pas d'exhaustivité possible** :
  - Les schémas recensés sont uniquement issus de **cas connus**.
  - Les fraudes non découvertes restent **hors radar**.
- **Évolution constante des techniques** :
  - L'usage des technologies (deepfake, crypto, IA) renforce la complexité.
  - Les fraudeurs s'adaptent aux dispositifs de prévention : effet de **contre-innovation**.
- **Imagination sans limite** :
  - Certains montages sont créés sur mesure pour une cible ou une faille spécifique.
  - Les fraudeurs testent les limites du système pour **y insérer leur stratagème**.
- **Message clé :** L'objectif n'est pas de tout prévoir, mais d'identifier les **logiques récurrentes** pour anticiper les dérives.

Comprendre la fraude pour mieux la prévenir

Objectif de cette partie,

Fournir une grille de lecture structurée pour :

- Identifier les **principaux schémas de fraude interne et externe**,
- Comprendre **les mécanismes typiques utilisés**,
- Sensibiliser aux **risques associés à chaque processus de gestion**.
- **une approche par processus ?**
- La fraude ne surgit pas de nulle part : elle s'infiltre dans **les flux opérationnels existants**.

Un raisonnement par processus :

  - permet de **visualiser les zones de vulnérabilité**,
  - facilite l'adaptation des contrôles à la réalité des activités,
  - **standardise l'analyse** pour des structures de toutes tailles (PME, administration, grands groupes).

- **Impact de la fraude**
- **Pertes financières importantes** (liquidité, actifs, chiffre d'affaires).
- **Atteinte à la réputation** (perte de crédibilité, mauvaise presse).
- **Risque de perte de confiance** des parties prenantes : clients, fournisseurs, personnel, régulateurs.

Limites de l’analyse et périmètre

- **Schémas fondés sur des cas réels**
- Les typologies analysées dans ce module sont issues de **dossiers judiciaires, rapports d’audit et retours terrain**.
- Il s’agit d’**exemples représentatifs**, mais **pas d’un catalogue complet** de toutes les fraudes possibles.
- **Les fraudeurs innovent constamment**
- Les techniques évoluent au rythme des nouvelles technologies (IA, failles cloud, anonymisation…).
- Les fraudeurs s’adaptent aux contrôles mis en place et exploitent **les angles morts du système**.
- **Une approche formatrice, non prescriptive**
- L’objectif n’est **pas de donner des recettes**, mais de :
  - **développer la capacité à repérer les signaux faibles** ;
  - former à une **posture de vigilance** et d’analyse critique ;
  - favoriser **l’anticipation plutôt que la réaction**.
- **Visuel suggéré**
- Un **cerveau stylisé** connecté à des pièces de puzzle représentant :
  - **innovation** (ampoule, technologie),
  - **complexité** (pièces non alignées),
  - **inconnu** (zone grisée),
- Représente la **mobilisation de l’intelligence collective face à l’inventivité frauduleuse**.

Méthodologie de présentation

Une étude fondée sur les processus de gestion

- L’analyse est organisée **par processus clé** (achats, ventes, trésorerie, etc.).
- Chaque processus fera l’objet :
  - d’une **présentation des risques typiques**,
  - de **cas illustrés issus de faits réels**,
  - de **check-lists d’indicateurs d’alerte**.
- **Double objectif**
- **Sensibiliser** les parties prenantes aux risques concrets de fraude.
- **Outiller** les professionnels pour détecter, prévenir et documenter les anomalies.

  - Achats → Stock → Production → Ventes → Trésorerie → Paie.

Pourquoi raisonner par processus ?

1. Un schéma clair et reproductible,

- Un **processus** est une suite logique d'étapes (commande, validation, exécution, paiement…).
- Cette structuration permet de **découper les flux opérationnels**, d'identifier les points d'entrée et de sortie de l'information ou des fonds.
- **2. Visualisation directe des flux à risque,**
- La fraude s'infiltre souvent dans les **interstices entre deux étapes**.
- Une cartographie par processus permet de **repérer les ruptures de contrôle**, les validations automatiques, les zones non supervisées.
- **3. Une approche transversale applicable à tous les secteurs**
- Qu'il s'agisse d'un ministère, d'une association, d'une entreprise publique ou privée, les grands processus restent similaires.
- **Avantage : reproductibilité de l'analyse** dans des environnements variés.

👉 **Schéma à flèches linéaires** représentant le flux d'un processus :

- **Input → Traitement → Output**,
- Exemple : Demande d'achat → Bon de commande → Livraison → Facture → Paiement.

Les 5 processus fondamentaux à surveiller

- **Processus les plus exposés à la fraude :**
- **Achats** : fournisseurs fictifs, fausses factures, surfacturation.
- **Ventes** : détournement de règlements, lapping, fausses ventes.
- **Trésorerie / Caisse** : skimming, faux rapprochements bancaires.
- **Stocks & immobilisations** : sorties non autorisées, vols dissimulés.
- **Paie & frais** : salariés fictifs, remboursements indues, variables manipulées.
- **Pourquoi ceux-là ?**
- Ce sont les **nœuds de flux financiers ou de valeurs**.
- Ils impliquent souvent une **chaîne de responsabilités** (commanditaire, valideur, exécuteur), donc des risques de **connivence ou de défaillance**.

Cartographie des détournements d’actifs

- **Typologie des détournements internes**
- Le schéma général des fraudes internes montre que les détournements :
  - S’opèrent **au sein des processus eux-mêmes** (ex : achat → paiement),
  - Sont facilités par **l’absence ou la faiblesse de contrôle à certains points clés**.

Exemples de mécanismes par processus

Processus	Exemple de fraude typique	Signal d’alerte
Achats	Fournisseur fictif	Pas de bon de commande
Ventes	Détournement de chèque client	Absence d'encaissement
Trésorerie	Faux rapprochement bancaire	Écarts inexpliqués
Stocks	Vol dissimulé lors des retours SAV	Stock physique ≠ théorique
Paie	Salarié fantôme / Double remboursement	Anomalies dans les historiques

Pourquoi le processus achat est-il sensible ?

Un point de sortie direct de la trésorerie

- Chaque achat validé débouche sur un **paiement**, ce qui en fait **un vecteur de sortie d'argent** critique.
- La fraude à ce niveau permet **un enrichissement personnel immédiat**.

Des failles structurelles fréquentes

- Absence ou faiblesse de **segmentation des fonctions** (demandeur = valideur = payeur).
- Manque de **référentiel fournisseurs** à jour ou de **vérifications préalables**.

- **Chaîne illustrée** : Commande → Réception → Facture → Paiement, avec pictogrammes de rupture potentielle à chaque étape.

Fausse facture – Mécanisme global

Schéma classique en 3 temps

- **Création d’un fournisseur fictif** ou réutilisation d’une structure existante.
- **Émission d’une facture** sans livraison réelle.
- **Paiement effectué** sans contrôle effectif ni contrepartie.

Objectif : détourner des fonds sans éveiller les soupçons.

Points de faiblesse – Fournisseur fictif

- **Signaux d’alerte typiques**
- Pas de pièce justificative : **pas de RC, RIB non vérifié, pas de contrat**.
- Fournisseur récemment réactivé après **longue inactivité**.
- Adresse suspecte ou **données génériques (gmail, boîte postale, etc.)**.

Points de faiblesse – Facture fictive

- **Anomalies classiques**
- Description vague ou générique du service rendu.
- Montant élevé sans **bons de commande ni réception associée**.
- Facture **isolée, urgente ou exceptionnelle**, souvent réglée en contournant la procédure.

Récupération du paiement

- **Comment l'argent est-il détourné ?**
- Par **virement sur un compte externe** contrôlé par le fraudeur.
- Par **chèque encaissé sur un compte personnel ou dormant**.
- **Absence de liasse documentaire complète** au moment du paiement.

👉 **Circuit de paiement** illustré (ordre de paiement → compte bancaire → bénéficiaire réel),

Étude de cas – Cryospace

Contexte

- Société victime d’un détournement de **13 M€ via fausses prestations**.
- Création de **prestataires fictifs avec entités existantes recyclées**.

- 🕑 **Chronologie résumée**
- Étape 1 : Connivence d’un agent avec fournisseur.
- Étape 2 : Contrats simulés + validation interne.
- Étape 3 : Règlements réguliers pendant plusieurs mois.

Paiement en double

- **Technique fréquente**
- Réutilisation de la **même facture sous un format différent** (PDF, impression, numérotation proche).
- Fraude sur les **documents scannés ou mal indexés**.
- Souvent détectée par **audit externe** ou erreur de trésorerie.

Falsification de moyens de paiement

Exemples de falsification

- **Chèques falsifiés** (modification du montant ou du bénéficiaire).
- **Virements détournés** vers un compte masqué.
- Masquage par **comptes de contrepartie** ou **comptabilité parallèle**.

Autres fraudes rattachées aux achats

- **Typologies diverses**
- **Faux crédits fournisseurs** : exagération des ristournes ou avoirs à verser.
- **Fausses bourses / aides détournées** dans les administrations.
- Manipulation des **dossiers d’attribution ou d’exonération.**

👉 **dossiers administratifs + cachets fictifs**, institutions détournées.

Check-list “Achats” – Contrôles clés

- **Contrôles à systématiser**
- Existence d’un **bon de commande signé**.
- Présence d’une **preuve de réception effective**.
- Vérification du **référentiel fournisseur** (KYC complet).
- Analyse des **paiements doublons ou atypiques**.

- 📊 **Indicateurs de détection**
- Taux de **commandes hors procédure**.
- Nombre de **fournisseurs à facturation unique**.
- Écarts entre **montant budgété et engagé**.

Risques liés aux ventes à crédit

Des enjeux financiers majeurs.

- La vente n’est pas finalisée tant que le **paiement client n’est pas encaissé**.
- Les systèmes de crédit client (délais de paiement, remises, ristournes) ouvrent des **zones grises de manipulation**.

Des responsabilités partagées

- Les ventes impliquent plusieurs intervenants : commerciaux, comptabilité, recouvrement.

Cela multiplie les **risques de collusion ou de déresponsabilisation**.

👉 Commande → Livraison → Facturation → Encaissement.

Détournement de chèques clients

- **Mécanisme typique**
- Le client règle par **chèque nominal ou virement**.
- L'agent détourne ce paiement :
  - soit en **encaissant le chèque sur un compte personnel**,
  - soit en **ne l'enregistrant jamais**.

- 🚩 **Signal d'alerte : absence de relance**
- Le client considère avoir payé → ne relance pas.
- L'organisation pense que la créance est toujours active → **trou dans la trésorerie**.

Le Lapping – Transfert de compte

Définition

- Détournement temporaire de paiement d'un client A, **caché par l'encaissement ultérieur du client B**, etc.

Effet domino

- Repose sur un **flux permanent de nouveaux paiements** pour masquer les précédents.
- Découvert souvent **trop tard**, à l'occasion d'un audit ou d'un défaut de paiement.

- 👉 **3 flèches croisées** A → B → C, avec encaissements croisés.

Fraudes sur facturation

- **Techniques fréquentes**
- **Sous-facturation volontaire** au profit de proches ou d'un tiers complice.
- **Sur-facturation** : le trop-perçu est détourné, ou justifié fictivement.
- **Facturation en contournement de client** (vol de clientèle).

👉 3 flèches comparatives :
  - Prix réel,
  - Prix facturé,
  - Montant réellement encaissé.

Client fictif – Objectif de surévaluation

- **Pourquoi créer un client fictif ?**
- Pour gonfler artificiellement :
  - les **volumes de vente**,
  - les **primes de performance**,
  - les **résultats comptables**.

- **Impact sur la sincérité des états financiers**
- Représente une **fraude intellectuelle grave**, souvent couplée à une fraude comptable.

Relance & circularisation : outils de contrôle

Méthodes efficaces

- **Relance client** régulière : détecte les encaissements non suivis.
- **Circularisation directe** par l'auditeur (confirmation de solde client).

🔍 **Avantage**

- **Bypasse l'interne** : vérification indépendante.
- Permet de **valider l'existence réelle de la créance**.

Check-list “Ventes” – Contrôles essentiels

Contrôles clés

- Existence d’une **commande validée**.
- Concordance : **livraison ↔ facturation ↔ encaissement**.
- Suivi des **clients à facturation unique** ou dormant.
- Analyse des **avoirs, remises inhabituelles, annulations**.

📊 **Indicateurs de fraude potentielle**

- Taux d’impayés / retards anormaux.
- Variation brusque des ventes en fin de période.
- Clients sans identifiant fiscal / email générique.

Signes à surveiller dans les ventes

Signaux d’alerte comportementaux ou documentaires

- Pression pour “clôturer vite” des ventes.
- Factures **hors canal normal / urgence exceptionnelle**.
- Absence de justificatif de livraison.
- **Clients non répondants à la circularisation**.

Enjeux et vulnérabilités de la trésorerie

Pourquoi la trésorerie est-elle exposée ?

- C’est le **centre nerveux financier** de toute organisation.
- Elle regroupe les flux **liquides et traçables** (espèces, chèques, virements), et donc attire les fraudeurs.

Vulnérabilités fréquentes

- **Manque de séparation des fonctions** (encaissement, saisie, rapprochement).
- **Rapprochements bancaires négligés** ou absents.
- Faible digitalisation dans certaines structures.

Skimming – L’écrémage des recettes

Définition

- L’agent **encaisse une vente sans l’enregistrer** dans le système.
- Fréquent dans les environnements à **paiement en espèces** (billetterie, caisses de musées, guichets…).

Détection difficile

- Surtout si le ticket ou la trace numérique est absente.
- **Incohérences de caisse** ou marges anormalement faibles sont des indices.

Erreurs de caisse & annulations fictives

Techniques utilisées

- L’agent **annule une vente** après encaissement, mais garde l’argent.
- Il génère des **tickets “test”** ou des erreurs simulées.

⚠ **Apparence d’exactitude**

- Les montants semblent comptablement justes… mais les fonds sont détournés.

Détournement de dépôts bancaires

- **Mécanisme typique**
- Le dépôt de la recette du **jour 1 est détourné**, remplacé le lendemain par celui du jour 2 (“recyclage”).
- Les recettes sont **décalées artificiellement** pour masquer un trou de trésorerie.

🧠 **Fraude temporaire mais risquée**

- Peut durer des semaines si les montants varient peu d’un jour à l’autre.

Le Kitting – Surévaluation fictive de trésorerie

Définition

- Mécanisme consistant à **faire apparaître un solde bancaire artificiellement élevé** via des virements croisés entre comptes.

🧩 **Comment ça fonctionne**

- Virement émis **juste avant clôture** mais non réellement encaissé,
- **Apparence de solvabilité** temporaire (souvent en fin d’exercice).

Risques en magasin et billetterie

- **Fraudes fréquentes**
- **Ventes hors système** (billets non scannés, produits non passés en caisse).
- **Pannes simulées** (imprimantes, TPE) pour justifier l’absence de ticket.

Indicateurs à surveiller – Trésorerie

Alertes quantitatives

- **Démarque inconnue** (écart entre recettes théoriques et réelles).
- **Variations anormales** des flux de caisse.
- Taux élevé d'**annulations ou de retours en espèces**.

👉

Radar de contrôle avec 4 axes : Démarque – Flux – Annulations – Moyens de paiement.

Contrôles clés – Trésorerie & caisse

- **Mesures recommandées**
- **Rapprochement bancaire régulier**, signé par un supérieur.
- **Audit inopiné de caisse**.
- **Numérotation automatique et non modifiable des tickets**.
- **Séparation stricte** entre encaissement, comptabilisation, et dépôt.

Focus : falsification des rapprochements bancaires

Technique utilisée,

- Création de **faux extraits de banque**,
- **Saisie manuelle** ou modification des rapprochements dans le logiciel comptable.

🎯 **Objectif**

- Dissimuler un détournement ou **masquer une fraude dans les soldes**.

🔍 **Méthodes de détection**

- **Circularisation directe des banques**,
- **Analyse des soldes de fin de période** vs mouvements réellement comptabilisés.

Nature des risques liés aux stocks et immobilisations

Pourquoi ces postes sont-ils à risque ?

- Les stocks et immobilisations sont des **éléments physiques, transportables, revendables**.
- Ils peuvent être **manipulés, volés, remplacés ou mal enregistrés**.

🚨 **Risques spécifiques**

- Vols internes déguisés en pertes ou casses.
- **Usage personnel d'actifs** (véhicules, ordinateurs, outils…).
- Création d'**immobilisations fictives** pour détourner des fonds.

Schémas courants de fraude sur les stocks

- **Techniques observées**
- **“Sortie par la poubelle”** : produits dissimulés dans les déchets pour être récupérés ensuite.
- **Retours simulés** non enregistrés, mais récupérés.
- **Détournement d’objets réparés ou mis au rebut**.

📉 **Effet**

- Baisse artificielle du stock théorique,
- **Appauvrissement de l’inventaire physique**, sans justification valable.

Inventaire : un contrôle-clé souvent négligé

- **Problème fréquent**
- L’inventaire physique n’est pas toujours :
  - exhaustif,
  - contradictoire,
  - ou **réconcilié avec le stock comptable**.

📉 **Risques**

- Laisser passer des vols ou des pertes déguisées.
- Fausses écritures de régularisation pour **couvrir une fraude passée**.

Études de cas – Stocks détournés

Exemples notables

- **Galeries ABC** : vols organisés dans les entrepôts par des employés.
- **SAV** : revente de produits réparés prétendument “cannibalisés”.

🎯 **Technique commune :**

- Détournement sous couvert de **procédures internes insuffisamment surveillées**.

Immobilisations fictives ou utilisées à des fins personnelles

Formes fréquentes

- Création d'immobilisations **jamais livrées ou inexistantes** (machines, logiciels, équipements).
- Détournement d'un véhicule ou ordinateur affecté à un usage **personnel**.

📜 **Couverture comptable**

- Masquage via amortissement, immobilisation "en cours" non suivie, ou absence de vérification physique.

Check-list “Stocks & Immobilisations”

Contrôles à renforcer

- Inventaire annuel **contradictoire** et **documenté**.
- Contrôle des **mouvements physiques de stock** : entrées / sorties / pertes.
- Suivi des **immobilisations sur le terrain** (inventaire physique vs comptable).
- Validation préalable des acquisitions par **deux niveaux hiérarchiques distincts**.

📊 **Indicateurs à surveiller**

- Écarts d’inventaire non expliqués.
- Actifs “en cours d’acquisition” depuis plus d’un an.
- Taux de casse ou perte anormalement élevé.

Risques spécifiques au processus paie

- **Pourquoi la paie est-elle un processus critique ?**
- Elle représente **un flux régulier, stable et massif**, souvent peu audité.
- Les **données de paie sont complexes, sensibles** et difficiles à vérifier en détail.

🔒 Vulnérabilités fréquentes

- Accès excessif aux systèmes de paie (RH ou IT).
- Confiance aveugle dans les automatisations.
- Faible séparation entre **gestion RH** et **exécution de la paie**.

Le salarié fantôme

Mécanisme classique

- Création d’un **matricule salarié fictif** dans le logiciel.
- Versement mensuel d’un salaire vers **un compte contrôlé par le fraudeur**.

📂 **Variantes**

- Réactivation d’un contrat clôturé.
- Emploi de **faux papiers ou d’un nom réel d’ex-employé**.

Emploi fictif et double paiement

🧑💼 Deux schémas typiques

- Emploi fictif : **aucune activité réelle**, mais fiche de paie alimentée.
- Double paie : **doublon volontaire** dans les variables ou primes.

📑 Souvent liés à un contexte politique ou administratif

- Attribution de postes à des proches ou collaborateurs inexistants

Falsification des variables de paie

Variables sensibles

- Heures supplémentaires,
- Primes exceptionnelles,
- Congés payés ou récupérations non utilisés,
- Commissions.

🚩 **Manipulation possible**

- Intervention directe dans le fichier avant édition de la paie.
- Connivence avec le supérieur hiérarchique pour validation fictive.

Frais professionnels – Un classique de la fraude douce

Techniques fréquentes

- **Doublon de justificatif** sur plusieurs notes.
- **Justificatif modifié ou faux (tickets restaurants, hôtels)**.
- Frais engagés pour un usage personnel, **requalifiés en mission**.

📉 **Effet cumulé**

- Impact modéré unitairement, mais important dans le temps.

Check-list "Paie" – Contrôles essentiels

Points de contrôle recommandés

- **Journal des modifications du fichier paie** (traces d'ajouts récents).
- Concordance entre **registre RH et logiciel de paie**.
- Validation externe des primes, frais, variables.
- **Absence d'accès en écriture** des mêmes personnes en RH et paie.

📊 **Indicateurs à suivre**

- Salariés sans badgeage / sans activité projetée.
- Taux de primes / frais par rapport à la masse salariale.
- Créations de fiches dans les 5 jours avant paie.

séparation des fonctions RH / Paie

Principe fondamental de sécurité

- **La personne qui recrute ne doit pas être celle qui paie.**
- La saisie RH doit être validée par un **tiers indépendant** (Direction, Contrôle de gestion).

🧩 **Organisation recommandée**

- **RH** : gère les contrats, absences, changements.
- **Comptabilité / Finances** : exécute le paiement.
- **Audit interne** : supervise et contrôle.

Typologie des fraudes externes

Définition

- Les fraudes externes sont commises **par des entités extérieures à l'organisation**, parfois avec la complicité d'agents internes.

🧨 **Principales catégories**

- **Corruption** : obtention d'avantages indus contre rémunération occulte.
- **Escroquerie** : manipulation, mensonge ou abus de confiance.
- **Cybercriminalité** : intrusion, vol de données, falsification numérique.
- **Usurpation** : usurpation d'identité ou de rôle (ex. "faux président").

Corruption – Achats et surfacturation

- **Exemples typiques**
- Un acheteur accorde un marché à une entreprise **en échange d'un pot-de-vin**.
- Prix volontairement **gonflés** ou prestations inutiles commandées.

💣 Conséquences

- Appauvrissement de l'organisation,
- Risque pénal pour les deux parties,
- Atteinte à la transparence et à la gouvernance.

Escroqueries et Fraude au président

📞 Le scénario de l'urgence

- Un escroc se fait passer pour un dirigeant ou un cadre :
  - Il appelle en **urgence**, évoquant un virement confidentiel,
  - Il demande à **contourner les procédures habituelles**.

🧠 Moyens utilisés

- Ingénierie sociale,
- Usurpation vocale ou écrite,
- Stress et pression pour éviter la vérification.

Faux RIB et arnaques aux coordonnées bancaires

- **Technique**
- Le fraudeur transmet un **faux relevé d’identité bancaire** en se faisant passer pour un fournisseur existant.
- Le virement part vers **un compte contrôlé par l’escroc**.

⚠ **Souvent suite à un piratage de boîte mail ou par usurpation d’un email.**

Conflits d’intérêts et sociétés écrans

⚠️ Mécanisme

- Un agent passe des commandes ou accorde des contrats à :
  - **Une société qu’il contrôle directement**, ou
  - **Une société d’un proche / complice**.

🧩 Usage fréquent de sociétés écrans

- Sociétés sans activité réelle, parfois immatriculées à l’étranger,
- Opacité du capital ou fausses déclarations.

👉 Trois blocs “Société A – Société B – Agent interne” avec **flèches croisées**,

- Mise en évidence d’un **conflit d’intérêt dissimulé**

Check-list “Fraudes externes” – Prévention et détection

Procédures essentielles

- **Vérification systématique des coordonnées bancaires**, par un canal indépendant (téléphone direct).
- Mise à jour du **référentiel fournisseurs** après contrôle documentaire.
- **Charte anticorruption** signée par les agents exposés.
- **Canal d’alerte interne** pour les signalements anonymes.

📊 **Indicateurs à suivre**

- Fréquence des **changements de RIB**,
- Montants anormaux ou exceptionnels,
- Fournisseurs à **adresse générique ou étrangère**.

Intercepter le chèque

Encaisser

Dissimuler la disparition

Créer un fournisseur fictif

Créer une documentation fictive

Insérer dans le circuit de paiement

Récupérer le paiement

Facture réelle

Réutiliser la documentation

Insérer dans le circuit de paiement

Paiement en double

FOURNISSEUR

Récupérer le paiement en double

MERCI