

GUIDE PRATIQUE

ÉDITION 2026



MAÎTRISE DU RISQUE & CONFORMITÉ

Gérer les risques de fraude d'entreprise

Un guide pratique pour comprendre, cartographier, détecter et maîtriser la fraude — appuyé sur les référentiels ACFE, IIA et CFCA.

AUTEUR

TRIUM Solutions & Consulting SARL

Douala, Cameroun · RAFM Academy



TRIUM Solutions & Consulting SARL

RISK · AUDIT · REVENUE ASSURANCE & FRAUD MANAGEMENT

Gérer les risques de fraude d'entreprise

Guide pratique — Édition 2026

ÉDITEUR & AUTEUR

TRIUM Solutions & Consulting SARL

CONTACT

contact@rafmacademy.com

RÉFÉRENTIELS MOBILISÉS

ACFE — Association of Certified Fraud
Examiners

IIA — The Institute of Internal Auditors

CFCA — Communications Fraud Control
Association

VERSION

1.0 — Juin 2026

Document de référence interne

© 2026 TRIUM Solutions & Consulting SARL. Tous droits réservés. Cet ouvrage est protégé par le droit de la propriété intellectuelle. Toute reproduction, représentation ou diffusion, intégrale ou partielle, par quelque procédé que ce soit, sans autorisation écrite préalable de l'éditeur, est interdite. Les statistiques citées proviennent de sources publiques (ACFE *Report to the Nations*, enquêtes CFCA *Global Fraud Loss Survey*, cadres de l'IIA) et sont reproduites à titre informatif. Ce guide ne constitue pas un avis juridique ; il vise à fournir un cadre méthodologique.

Pourquoi ce guide

La fraude n'est plus un risque marginal. Elle s'est industrialisée, professionnalisée et accélérée à la faveur de la transformation numérique. Aucune organisation — entreprise privée, établissement public, opérateur de télécommunications ou institution financière — n'est aujourd'hui à l'abri.

Les chiffres parlent d'eux-mêmes. Les organisations perdent en moyenne près de **5 % de leur chiffre d'affaires annuel** du fait de la fraude professionnelle, et la fraude télécoms à elle seule représentait plus de **41 milliards de dollars** de pertes mondiales en 2025. Derrière ces montants se cachent des défaillances de contrôle, des signaux faibles ignorés et, trop souvent, une culture du risque insuffisamment ancrée.

Ce guide a été conçu par **TRIUM Solutions & Consulting** pour offrir aux dirigeants, auditeurs

internes, *risk managers* et responsables conformité un cadre clair et actionnable. Il ne se veut ni un traité académique, ni un catalogue de bonnes intentions, mais un outil de travail.

Nous y mobilisons trois référentiels de référence : les travaux de l'**ACFE** sur la fraude professionnelle, le cadre de maîtrise des risques de l'**IIA**, et les enquêtes de la **CFCA** sur la fraude dans les communications. Vous y trouverez des définitions, des statistiques actualisées, des schémas, des cartographies et des check-lists directement transposables à votre organisation.

La maîtrise de la fraude n'est pas qu'une affaire de contrôle : c'est un avantage compétitif. Une organisation qui détecte vite, réagit bien et apprend de ses incidents protège sa valeur, sa réputation et la confiance de ses parties prenantes. C'est l'ambition de ce guide.

« On ne maîtrise que ce que l'on mesure, et l'on ne détecte que ce que l'on a appris à voir. »

Sommaire

01	Comprendre la fraude	06
	Définitions, mécanismes et panorama des typologies	
02	Statistiques & tendances 2024–2026	11
	Les chiffres clés de l'ACFE et de la CFCA	
03	Le triangle de la fraude	17
	Pression, opportunité, rationalisation — et au-delà	
04	Typologies détaillées	22
	L'arbre de la fraude : détournement d'actifs, corruption, états financiers	
05	Le dispositif de contrôle interne	28
	Le modèle des trois lignes de l'IIA	
06	Cartographie & évaluation des risques	34
	Identifier, coter et prioriser le risque de fraude	
07	Détection : data analytics & red flags	40
	Signaux d'alerte, lignes d'éthique et analyse de données	
08	Fraude télécoms & RAFM	46
	Le cadre CFCA appliqué aux opérateurs	
09	Plan d'action & réponse à incident	51
	Du programme anti-fraude à la gestion de crise	
10	Boîte à outils	56
	Check-lists, glossaire et références	

Comment utiliser ce guide

1

Comprendre avant d'agir

Les chapitres 1 à 4 posent le vocabulaire commun et les mécanismes. Indispensables pour aligner direction, audit et opérationnels.

2

Construire le dispositif

Les chapitres 5 à 7 détaillent la prévention, la cartographie des risques et la détection. C'est le cœur opérationnel du programme anti-fraude.

3

Réagir & outiller

Les chapitres 8 à 10 couvrent le cas spécifique des télécoms (RAFM), la réponse à incident et la boîte à outils prête à l'emploi.

REPÈRE

Les encadrés dorés signalent un point de vigilance ou une bonne pratique à retenir.

DONNÉES

Les blocs chiffrés s'appuient sur des sources publiques citées en fin d'ouvrage.

SCHÉMA

Les diagrammes peuvent être repris dans vos supports internes de sensibilisation.

CHAPITRE

01

Comprendre la fraude

Avant de prévenir et de détecter, il faut nommer. Ce chapitre établit le vocabulaire commun, les mécanismes de la fraude et un panorama des grandes familles.

Définition

Panorama

Impacts

Une tromperie intentionnelle pour un gain indu

La fraude se définit comme tout **acte intentionnel de tromperie** visant à obtenir un avantage injuste ou illégal, ou à priver une victime d'un droit. Elle se distingue de l'erreur par le caractère délibéré de l'acte, et de la simple négligence par la volonté de dissimulation. L'ACFE qualifie plus précisément la **fraude professionnelle** (*occupational fraud*) comme l'usage de sa fonction pour s'enrichir par le détournement ou le mauvais usage délibéré des ressources de l'organisation.

LES TROIS CRITÈRES JURIDIQUES

Élément matériel — un acte de tromperie ou de dissimulation.

Élément intentionnel — la volonté de tromper.

Préjudice — un dommage ou un gain indu.

À NE PAS CONFONDRE

Erreur — non intentionnelle, corrigible.

Abus — usage excessif mais sans tromperie.

Fraude — intention + dissimulation + préjudice.

Fraude interne, externe et mixte

On distingue la **fraude interne**, commise par un collaborateur ou un dirigeant ; la **fraude externe**, commise par un tiers (client, fournisseur, cybercriminel) ; et la **fraude en collusion**, qui combine acteurs internes et externes — la plus difficile à détecter, car elle contourne la séparation des tâches.

Repère — La fraude n'est pas un événement isolé mais un *processus* : opportunité, passage à l'acte, dissimulation, puis souvent escalade. C'est cette dynamique que le dispositif de contrôle doit interrompre le plus tôt possible.

Les grandes familles de fraude

L'ACFE structure la fraude professionnelle en trois catégories. Elles diffèrent fortement par leur fréquence et par leur coût médian.

Détournement d'actifs

Vol ou usage abusif des ressources : décaissements frauduleux, fausses factures, notes de frais gonflées, vol de stocks, détournement de recettes.

89%

DES CAS

120 K\$ médian

Corruption

Abus d'influence dans une transaction : pots-de-vin, commissions occultes, conflits d'intérêts, favoritisme, ententes avec des tiers.

48%

DES CAS

200 K\$ médian

Fraude aux états financiers

Manipulation comptable : surévaluation du chiffre d'affaires ou des actifs, dissimulation de passifs, comptabilisation fictive. Rare mais dévastatrice.

5%

DES CAS

766 K\$ médian

38%

des dossiers combinent **au moins deux catégories** à la fois. Le chevauchement le plus fréquent associe détournement d'actifs et corruption : un signe que les fraudeurs élargissent leur champ d'action dès qu'une faille persiste.

Source : ACFE, *Occupational Fraud 2024: A Report to the Nations* (proportions de cas et pertes médianes ; la somme des catégories dépasse 100 % en raison des cas multiples).

Bien au-delà des sommes détournées

~5%

du chiffre d'affaires annuel perdu en moyenne par les organisations du fait de la fraude professionnelle.

12 mois

durée médiane avant qu'une fraude ne soit détectée — un an de pertes silencieuses.

145 K\$

perte médiane par dossier de fraude professionnelle, tous secteurs confondus.

3,1 Md\$

pertes totales documentées par l'ACFE sur 1 921 cas dans 138 pays.

Les coûts cachés

- Atteinte à la **réputation** et perte de confiance des clients et investisseurs.
- Coûts d' **enquête, de remédiation et de procédure** souvent supérieurs au montant détourné.
- Démotivation des équipes et **dégradation du climat éthique**
- Sanctions **réglementaires** et perte d'agréments dans les secteurs régulés.

Le profil-type contredit les idées reçues

Le fraudeur n'est pas un criminel d'habitude : dans la grande majorité des cas, il s'agit d'un collaborateur de confiance, sans antécédent.

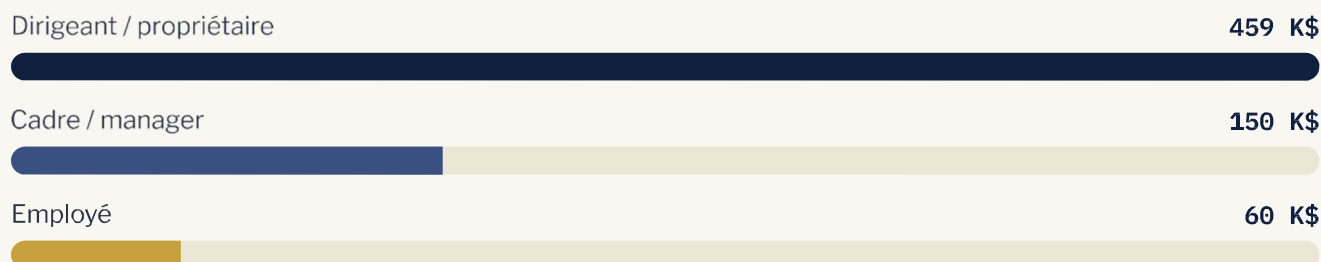
86%

des fraudeurs n'avaient **jamais été sanctionnés** auparavant pour des faits similaires.

+ d'ancienneté

plus le collaborateur est ancien et haut placé, plus la **perte médiane augmente**.

Le poste occupé change tout



Perte médiane selon le niveau hiérarchique de l'auteur — ACFE 2024. Largeur des barres relative au montant le plus élevé.

SIGNAUX COMPORTEMENTAUX FRÉQUENTS

Train de vie au-dessus des moyens, difficultés financières, refus de prendre des congés, relation anormalement étroite avec un fournisseur, contrôle jaloux de ses dossiers. Ces signaux faibles, présents dans la majorité des cas, doivent alerter avant même les chiffres.

De nouveaux vecteurs, une vitesse inédite

La transformation numérique a démultiplié la surface d'attaque. Les paiements instantanés, les canaux digitaux et l'intelligence artificielle générative offrent aux fraudeurs des leviers d'échelle et de crédibilité sans précédent — deepfakes vocaux, hameçonnage personnalisé, usurpation d'identité de masse.

Ingénierie sociale

Manipulation psychologique des collaborateurs pour contourner les contrôles : faux ordres de virement, « fraude au président », usurpation de fournisseurs.

IA & deepfakes

Clonage de voix de dirigeants et faux documents générés automatiquement, rendant les scénarios d'usurpation quasi indétectables à l'œil ou à l'oreille.

Paieement mobile

Dans les marchés africains, l'essor du *mobile money* crée des risques spécifiques : prise de contrôle de comptes, fraude au point de vente, blanchiment via agents.

LE PARADOXE DE LA MATURITÉ

Les mêmes technologies qui arment les fraudeurs renforcent aussi la défense : analyse de données en temps réel, apprentissage automatique, détection d'anomalies. La question n'est plus *si* l'organisation sera ciblée, mais à quelle vitesse elle saura voir, comprendre et réagir. C'est tout l'objet des chapitres suivants.

CHAPITRE

02

Statistiques & tendances 2024 – 2026

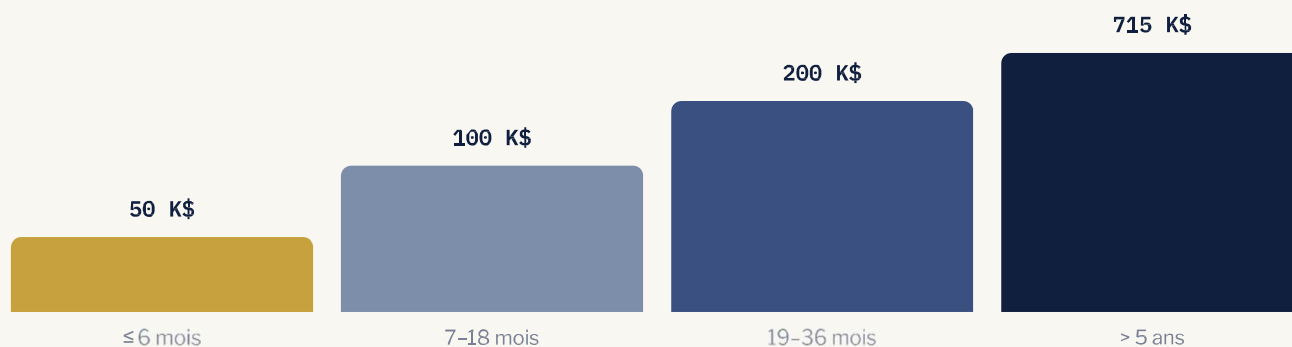
*Ce que disent les dernières enquêtes de l'ACFE et de la CFCA sur
l'ampleur, la détection et l'évolution de la fraude.*

L'ampleur en un coup d'œil

Synthèse du *Report to the Nations* 2024 de l'ACFE — la plus vaste étude mondiale sur la fraude professionnelle.



Durée de la fraude et ampleur de la perte



Lecture : plus une fraude dure, plus la perte médiane explose. La détection précoce est le premier levier d'économie. Ordres de grandeur d'après l'ACFE 2024.

Le signalement, première ligne de détection

Loin devant l'audit ou les contrôles automatisés, ce sont les **tips** — signalements humains — qui révèlent le plus de fraudes.



- **43%** Signalement (*tip*)
- **14%** Examen interne par le management
- **12%** Audit interne
- **12%** Découverte par hasard / autres
- **19%** Contrôles, rapprochements, audit externe...

D'OÙ VIENNENT LES SIGNALEMENTS

Employés	52%
Clients	21%
Anonyme	15%
Fournisseurs	11%

À RETENIR

Une organisation dotée d'une **ligne d'éthique** active détecte ses fraudes plus tôt et subit des pertes nettement inférieures. Le canal web est désormais le mode de signalement le plus utilisé, devant l'e-mail et le téléphone.

Source : ACFE, Report to the Nations 2024. Le signalement détecte environ trois fois plus de fraudes que la méthode suivante.

La défaillance des contrôles, cause n°1



>50%

des fraudes sont rendues possibles par une **absence ou un contournement de contrôles internes**. Autrement dit, plus d'une fraude sur deux était évitable par un dispositif de contrôle correctement conçu et appliqué.

82%

des organisations victimes ont **renforcé leurs contrôles** après l'incident — souvent trop tard.

84%

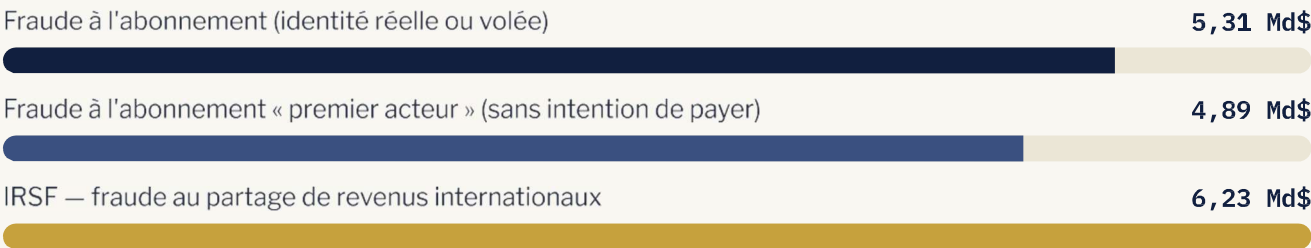
des victimes disposaient pourtant d'un **audit externe** des états financiers : un audit légal ne suffit pas à prévenir la fraude.

Une fraude qui accélère

Selon les enquêtes *Global Fraud Loss Survey* de la CFCA, les pertes mondiales liées à la fraude télécoms n'ont cessé de croître.



Top des fraudes par montant de perte (2023)



Sources : CFCA Global Fraud Loss Survey (2023, 2025). Le chapitre 8 est entièrement consacré à la fraude télécoms et au RAfM.

Sanction, recouvrement et récidive

68%

des fraudeurs ont été licenciés

57%

des cas transmis à la justice

72%

des poursuites aboutissent à
une condamnation

Le recouvrement reste l'exception

Malgré les sanctions, **la récupération des sommes détournées est rare et partielle**. Une part importante des organisations victimes ne recouvre jamais l'intégralité de leur préjudice. C'est l'argument économique décisif en faveur de la prévention : un euro investi dans le contrôle vaut bien davantage qu'un euro espéré au recouvrement.

POURQUOI SI PEU DE POURSUITES ?

Crainte du risque réputationnel, coût et durée des procédures, manque de preuves exploitables. D'où l'importance d'une enquête rigoureuse et documentée dès le premier soupçon.

LE COÛT DU SILENCE

Une part notable des fraudeurs non poursuivis récidive ailleurs. Ne pas sanctionner, c'est exporter le risque — et fragiliser la culture de l'intégrité en interne.

Cinq dynamiques à surveiller

01 L'IA générative au service des fraudeurs

Deepfakes vocaux et vidéo, e-mails d'hameçonnage rédigés sans fautes, faux documents : la barrière technique du fraudeur s'effondre.

02 La prise de contrôle de comptes (ATO)

Vol d'identifiants, SIM swapping et manipulation des parcours digitaux : la fraude se déplace de la technologie vers la **manipulation de l'identité**.

03 La fraude au paiement instantané

L'irrévocabilité des virements instantanés et du *mobile money* réduit à néant la fenêtre de rattrapage : la prévention devient l'unique rempart.

04 La pression réglementaire croissante

Lutte anti-blanchiment, protection des données, devoir de vigilance : les obligations se renforcent et la responsabilité des dirigeants s'élargit.

05 La défense par la donnée

En réponse, les organisations adoptent l'analyse continue, la détection d'anomalies et le scoring en temps réel. L'avantage va à celui qui exploite le mieux ses propres données.

CHAPITRE

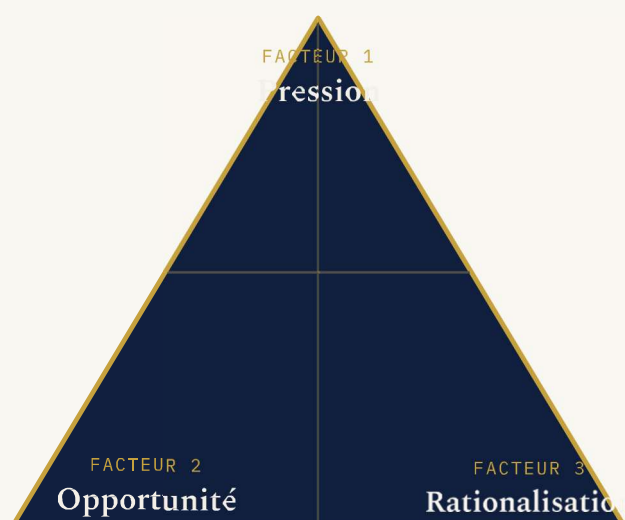
03

Le triangle de la fraude

Trois conditions doivent être réunies pour qu'une fraude survienne. Les comprendre, c'est savoir où agir.

Trois conditions, une seule fraude

Le criminologue Donald Cressey a montré que la fraude résulte de la conjonction de trois facteurs. Supprimez-en un, et la fraude devient improbable.



Pression / incitation

Un besoin financier perçu comme « non partageable » : dettes, addiction, objectifs intenable, train de vie.

Opportunité

Une faille dans les contrôles, un excès de confiance ou de pouvoir, qui rend l'acte possible sans être vu.

Rationalisation

La justification morale : « je le mérite », « je rembourserai », « l'entreprise ne s'en apercevra pas ».

Le levier de l'organisation — Pression et rationalisation relèvent de la sphère personnelle du fraudeur. L'**opportunité** est le seul angle sur lequel l'entreprise a une prise directe, par son dispositif de contrôle interne.

Reconnaître les signaux de chaque sommet

■ Pression — les déclencheurs

- Difficultés financières personnelles
- Addictions (jeu, substances)
- Maintien d'un train de vie
- Objectifs de performance irréalistes
- Pression hiérarchique sur les résultats
- Insatisfaction ou sentiment d'injustice

■ Opportunité — les failles

- Absence de séparation des tâches
- Contrôles inexistantes ou contournables
- Accès informatiques non revus
- Concentration des pouvoirs sur une personne
- Rapprochements bancaires non effectués
- Confiance aveugle dans un « homme clé »

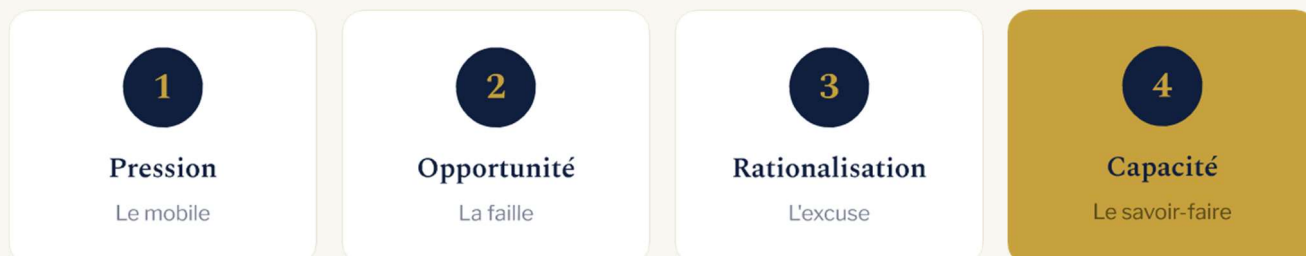
■ Rationalisation — les justifications

- « Ce n'est qu'un emprunt »
- « Tout le monde le fait »
- « Je rétablirai la situation »
- « On me doit bien ça »
- « L'entreprise est assez riche »
- « Ce n'est pas vraiment du vol »

La **culture d'éthique** (tone at the top, code de conduite, exemplarité des dirigeants) agit directement sur la rationalisation : elle rend la justification morale plus difficile et abaisse la probabilité de passage à l'acte.

Un quatrième sommet : la capacité

Le modèle a été enrichi pour intégrer la **capacité** de l'individu à commettre et dissimuler la fraude. Toutes les conditions peuvent être réunies, mais sans compétences ni position adéquates, la fraude reste théorique.



Ce que recouvre la « capacité »

- **Position** — un poste donnant accès aux actifs ou aux systèmes.
- **Intelligence & compétence** — comprendre et exploiter les failles de contrôle.
- **Confiance en soi / ego** — conviction de ne pas se faire prendre.
- **Gestion du stress** — mentir et dissimuler dans la durée.

Certains auteurs ajoutent un cinquième élément — l'**arrogance** — pour décrire les fraudes commises au sommet de la hiérarchie, là où le sentiment d'impunité est le plus fort. C'est précisément pour cela que les fraudes de dirigeants coûtent le plus cher.

Réduire l'opportunité, dissuader le passage à l'acte

PRÉVENIR

Séparation des tâches, contrôles d'accès, délégations de pouvoir, doubles signatures. On réduit la **faille**.

DÉTECTER

Lignes d'éthique, analyse de données, rapprochements, audits. On augmente la **perception du risque d'être pris**.

DISSUADER

Sanctions exemplaires, communication, culture d'intégrité. On agit sur la **rationalisation**.

L'équation de la dissuasion

Un fraudeur potentiel compare, consciemment ou non, le **gain attendu** au **risque d'être détecté et sanctionné**. Toute mesure qui augmente la probabilité de détection ou la sévérité de la sanction déplace cet arbitrage. Un dispositif visible et crédible dissuade donc *avant même* d'avoir à détecter quoi que ce soit.

Le reste de ce guide décline concrètement ces trois leviers : **prévenir** par le contrôle interne (chapitre 5), **détecter** par la cartographie et l'analyse (chapitres 6 et 7), et **réagir** par un plan d'action structuré (chapitre 9).

CHAPITRE

04

Typologies détaillées

L'arbre de la fraude de l'ACFE : une taxonomie complète des schémas, branche par branche.

L'arbre de la fraude professionnelle



Lecture — Le détournement d'actifs est le plus fréquent mais le moins coûteux par cas ; la fraude aux états financiers est l'inverse. La corruption se situe entre les deux et alimente souvent les deux autres branches.

La fraude la plus courante

Présente dans près de 9 dossiers sur 10. Souvent de faible montant unitaire, mais répétitive et durable.

Schémas sur la trésorerie

Vol direct d'espèces, *skimming* (détournement avant enregistrement), *larceny* (après enregistrement), encaissements non comptabilisés, fausses notes de crédit.

Décaissements frauduleux

Fournisseurs fictifs, fausses factures, double paiement, salariés fantômes sur la paie, notes de frais gonflées ou fictives, chèques falsifiés.

Actifs non monétaires

Vol de stocks et d'équipements, usage personnel des actifs, détournement de marchandises, fuite d'informations confidentielles.

SIGNAUX D'ALERTE

- Écarts de caisse ou d'inventaire récurrents
- Fournisseurs à adresse = celle d'un salarié
- Factures rondes, séquentielles, sans BC
- Avoirs et annulations anormalement fréquents

PARADES CLÉS

- Séparation commande / réception / paiement
- Référencement & KYC fournisseurs
- Rapprochements bancaires indépendants
- Inventaires tournants inopinés

La fraude en collusion

Elle implique presque toujours un tiers (fournisseur, client, agent), ce qui la rend difficile à détecter par la seule séparation des tâches.

Pots-de-vin & commissions occultes

Versements pour influencer une décision d'achat ou d'attribution. Souvent dissimulés en honoraires de conseil, frais de marketing ou surfacturation partagée.

Conflits d'intérêts

Un décideur a un intérêt personnel non déclaré dans une transaction : entreprise détenue par un proche, double emploi, favoritisme dans le recrutement.

Trucage d'appels d'offres

Ententes entre soumissionnaires, fuite d'informations, cahiers des charges taillés sur mesure, fractionnement des marchés pour éviter les seuils de contrôle.

SIGNAUX D'ALERTE

- Un fournisseur toujours retenu sans mise en concurrence
- Prix supérieurs au marché, qualité moindre
- Proximité inhabituelle acheteur / fournisseur
- Refus de rotation des fournisseurs

PARADES CLÉS

- Déclarations de conflits d'intérêts annuelles
- Mise en concurrence & seuils d'approbation
- Politique cadeaux & invitations
- Due diligence des tiers (anti-corruption)

Rare, mais la plus destructrice

Moins de 1 cas sur 20, mais une perte médiane plus de cinq fois supérieure à celle de la corruption. Elle émane presque toujours de la direction.

GONFLER LE RÉSULTAT

- Produits fictifs ou anticipés
- Ventes circulaires (channel stuffing)
- Surévaluation des stocks et actifs
- Capitalisation abusive de charges

MINORER OU DISSIMULER

- Passifs et provisions dissimulés
- Charges reportées sur l'exercice suivant
- Engagements hors bilan non révélés
- Annexes incomplètes ou trompeuses

Indicateurs à surveiller

- Croissance du résultat déconnectée des flux de trésorerie d'exploitation.
- Hausse anormale des créances clients ou des stocks.
- Écritures manuelles importantes en fin de période.
- Pression intense de la direction sur l'atteinte des objectifs.

Vigilance gouvernance — Parce qu'elle vient du sommet, cette fraude échappe aux contrôles opérationnels. Le rempart est ici la **gouvernance** : comité d'audit indépendant, audit interne rattaché au conseil, et culture qui autorise la remise en question des chiffres.

Quand la menace vient de l'extérieur

Fraude au virement (BEC)

Usurpation d'un dirigeant ou d'un fournisseur pour obtenir un virement vers un compte frauduleux. La « fraude au président » reste l'attaque la plus coûteuse pour les PME.

Hameçonnage & rançongiciel

Vol d'identifiants par e-mail piégé, puis prise de contrôle ou chiffrement des systèmes contre rançon.

Fraude au faux fournisseur

Demande de changement de RIB par un tiers se faisant passer pour un fournisseur connu, juste avant une échéance de paiement.

Usurpation & deepfake

Voix ou visage clonés par IA pour valider un faux ordre. La vérification par un second canal devient indispensable.

LE RÉFLEXE ANTI-BEC

Toute demande de virement urgent, de changement de coordonnées bancaires ou de confidentialité inhabituelle doit déclencher une **vérification par un canal différent** (rappel sur un numéro connu) et un **double contrôle**. Aucune urgence ne justifie de contourner la procédure.

Le fournisseur fantôme

Scénario reconstitué à des fins pédagogiques — toute ressemblance serait fortuite.

MOIS 1 – PRESSION

Le responsable achats, endetté, fait face à une difficulté financière personnelle qu'il ne peut partager.

MOIS 2 – OPPORTUNITÉ

Il référence seul les fournisseurs et valide les factures jusqu'à un seuil : aucune séparation des tâches. Il crée une société écran à son nom de jeune fille.

MOIS 3 À 14 – PASSAGE À L'ACTE

Des factures de « prestations de conseil » justes sous le seuil sont émises chaque mois. Il se rationalise : « je rembourserai dès que possible ».

MOIS 14 – DÉTECTION

Un collègue signale via la ligne d'éthique une adresse de fournisseur identique à celle d'un salarié. L'analyse de données confirme le schéma.

Les trois failles — absence de séparation des tâches, seuil de contrôle exploité, et référencement fournisseur non indépendant. Trois contrôles simples auraient interrompu le schéma dès le premier mois.

CHAPITRE

05

Le dispositif de contrôle interne

Prévenir plutôt que guérir : le cadre COSO et le modèle des trois lignes de l'IIA pour bâtir une défense robuste.

Cinq composantes, un système

Le référentiel COSO structure le contrôle interne en cinq composantes interdépendantes.

La fraude exploite toujours leur maillon le plus faible.

1

Environnement de contrôle

Le « ton donné par le sommet » : intégrité, valeurs éthiques, structure de gouvernance.

2

Évaluation des risques

Identifier et analyser les risques — dont le risque de fraude — qui menacent les objectifs.

3

Activités de contrôle

Politiques et procédures : séparation des tâches, autorisations, contrôles applicatifs.

4

Information & communication

Diffuser la bonne information, en interne et en externe, dont les canaux de signalement.

5

Pilotage & surveillance

Évaluer en continu l'efficacité du dispositif et corriger les défaillances.

Qui fait quoi face au risque

Le modèle de l'IIA clarifie les rôles dans la maîtrise des risques et évite les zones grises où la fraude prospère.

1^{re} ligne — Le management opérationnel

DÉTENIR LE RISQUE

Les équipes qui détiennent et gèrent le risque au quotidien. Elles appliquent les contrôles intégrés aux processus (autorisations, rapprochements, séparation des tâches).

2^e ligne — Les fonctions de surveillance

ENCADRER LE RISQUE

Risk management, conformité, contrôle interne, sécurité. Elles définissent le cadre, outillent la 1^{re} ligne et surveillent l'exposition (dont la fonction anti-fraude / RAFM).

3^e ligne — L'audit interne

ASSURANCE INDÉPENDANTE

Évaluation objective et indépendante de l'efficacité de la gouvernance, du management des risques et du contrôle. Rattachée au conseil / comité d'audit.

AU-DESSUS

L'**organe de gouvernance** (conseil, comité d'audit) supervise l'ensemble et fixe le ton.

EN DEHORS

Les **prestataires externes d'assurance** (auditeurs légaux, régulateurs) complètent le dispositif.

Trois familles de contrôles complémentaires

Préventif

Empêcher la fraude avant qu'elle survienne.

Séparation des tâches ·
Habitations · Doubles signatures
· Mots de passe · Référencement
des tiers

Détectif

Repérer la fraude qui a échappé à la prévention.

Rapprochements · Revues
analytiques · Ligne d'éthique ·
Audits · Détection d'anomalies

Correctif

Limiter l'impact et éviter la récurrence.

Enquête · Sanction ·
Recouvrement · Remédiation des
contrôles · Retour d'expérience

La séparation des tâches : le contrôle-roi

Aucune personne ne doit contrôler à elle seule toutes les étapes d'une transaction. Le principe : dissocier les fonctions d'**autorisation**, d'**exécution**, de **conservation** des actifs et d'**enregistrement** comptable.

Autoriser



Exécuter



Conserv



Enregistrer

Quatre fonctions, au moins deux personnes distinctes. En PME, où l'effectif limite la séparation, on compense par une revue renforcée de la direction.

Les piliers d'un programme structuré

Gouvernance & politique

Une politique anti-fraude validée par le conseil, un responsable désigné et un rattachement clair garantissent l'indépendance et l'autorité.

Code de conduite

Des règles claires sur les conflits d'intérêts, les cadeaux, les paiements et l'usage des actifs, signées par chacun.

Ligne d'éthique

Un canal de signalement confidentiel, multi-accès, protégeant le lanceur d'alerte. C'est le contrôle au meilleur rapport coût / détection.

Sensibilisation & formation

Former les collaborateurs à reconnaître et signaler la fraude. Une équipe avertie est le meilleur capteur de signaux faibles.

Diligence sur les tiers

Vérifier l'identité et l'intégrité des fournisseurs, agents et partenaires avant et pendant la relation.

Sanctions & exemplarité

Une réponse ferme et homogène à chaque cas avéré, communiquée pour son effet dissuasif — sans exception au sommet.

1/2

Les organisations dotées d'une ligne d'éthique et d'une formation anti-fraude détectent leurs fraudes plus tôt et subissent des pertes médianes **environ deux fois inférieures** à celles qui en sont dépourvues. La prévention n'est pas un coût, c'est un rendement.

L'assurance indépendante

Selon les normes de l'IIA, l'audit interne doit évaluer la probabilité de fraude et la manière dont l'organisation en gère le risque. Il n'est pas le premier responsable de la prévention — qui incombe au management — mais il en vérifie l'efficacité et alerte la gouvernance.

- **Évaluer** l'exposition au risque de fraude dans son plan d'audit fondé sur les risques.
- **Tester** la conception et l'efficacité des contrôles anti-fraude.
- **Rester vigilant** aux indices de fraude lors de chaque mission, avec un esprit critique.
- **Rendre compte** au comité d'audit en toute indépendance.

INDÉPENDANCE

Le rattachement fonctionnel au comité d'audit protège l'auditeur des pressions et garantit la liberté de ses constats.

LIMITE

L'audit interne apporte une assurance raisonnable, non absolue. La collusion et le contournement par la direction restent des angles morts à couvrir par la gouvernance.

CHAPITRE

06

Cartographie & évaluation des risques

Identifier, coter et prioriser le risque de fraude pour concentrer les contrôles là où ils comptent.

Évaluer le risque de fraude (FRA)

1

Identifier les scénarios de fraude

Par processus et par acteur : « qui pourrait frauder, comment, et en exploitant quelle faille ? » On s'appuie sur l'arbre de la fraude (chapitre 4).

2

Coter le risque inhérent

Évaluer la probabilité et l'impact de chaque scénario, avant prise en compte des contrôles existants.

3

Évaluer les contrôles existants

Cartographier les contrôles en place et juger leur efficacité réelle, pas seulement leur existence sur le papier.

4

Déterminer le risque résiduel

Risque inhérent atténué par les contrôles. C'est lui qui guide la priorisation et l'appétence au risque.

5

Traiter & suivre

Plans d'action sur les risques prioritaires, propriétaires désignés, échéances et revue périodique.

Probabilité × impact

Positionner chaque scénario sur une grille permet de visualiser les priorités d'un coup d'œil et de partager le diagnostic avec la direction.



Un outil de pilotage vivant

Le registre formalise chaque scénario, sa cotation, ses contrôles et son propriétaire. Modèle simplifié ci-dessous.

SCÉNARIO	PROCESSUS	INHÉR.	RÉSID.	CONTRÔLE CLÉ
Fournisseur fictif	Achats / P2P	Élevé	Moyen	KYC + séparation
Détournement de recettes	Encaissement	Moyen	Faible	Rapprochement quotidien
Corruption / appel d'offres	Marchés	Élevé	Moyen	Mise en concurrence
Fraude au virement (BEC)	Trésorerie	Élevé	Faible	Double canal + double validation
Salarié fantôme	Paie / RH	Moyen	Faible	Revue RH / paie croisée

Bonne pratique — chaque ligne doit avoir un **propriétaire nommé**, une **échéance** et un **statut**. Le registre se revoit au moins annuellement, et après tout incident ou changement majeur d'organisation.

Quatre stratégies de traitement

Réduire

Renforcer ou ajouter des contrôles pour abaisser probabilité et/ou impact. La stratégie par défaut pour les risques élevés.

Transférer

Partager le risque via une assurance fraude ou une clause contractuelle. Ne supprime pas le risque réputationnel.

Éviter

Renoncer à l'activité, au canal ou au partenaire trop risqué lorsque le risque résiduel reste inacceptable.

Accepter

Assumer consciemment un risque faible, en deçà de l'appétence définie, avec une simple surveillance.

Définir l'appétence au risque de fraude

Aucune organisation ne vise un risque nul — ce serait paralysant et ruineux. La gouvernance fixe une **appétence** : le niveau de risque résiduel acceptable. Tout ce qui dépasse ce seuil doit être traité ; ce qui reste en deçà est surveillé. C'est cette ligne qui rend les arbitrages explicites et défendables devant le conseil.

Piloter avec des KRI

Les *Key Risk Indicators* transforment la cartographie statique en surveillance continue.

Quelques exemples par domaine.

Achats

% de factures sans bon de commande · nombre de fournisseurs à paiement unique
· écarts de prix vs marché.

Trésorerie

nombre de changements de RIB fournisseurs · virements hors délais habituels ·
écritures manuelles.

RH / Paie

salariés sans congés sur 12 mois · comptes bancaires partagés · ajustements de
paie hors cycle.

Éthique

volume et délai de traitement des signalements · taux de complétion des
formations · conflits déclarés.

LE BON KRI

Un KRI utile est **mesurable, prédictif et doté d'un seuil d'alerte**. Trop d'indicateurs noient le signal ; mieux vaut une dizaine d'indicateurs suivis et discutés qu'un tableau de bord pléthorique jamais regardé.

CHAPITRE

07

Détection : data analytics & red flags

Voir tôt ce que les autres ne voient pas : signaux d'alerte, lignes d'éthique et analyse de données.

Apprendre à voir les signaux faibles

Aucun signal pris isolément ne prouve une fraude. C'est leur **accumulation** qui doit déclencher l'attention.

Signaux comportementaux

- Train de vie incompatible avec le salaire
- Refus systématique de congés ou de rotation
- Difficultés financières connues
- Lien anormalement étroit avec un tiers
- Réticence à partager ses dossiers

Signaux transactionnels

- Montants juste sous les seuils de contrôle
- Paiements ronds, séquentiels, dupliqués
- Tiers à coordonnées incohérentes
- Pics d'activité en fin de période
- Écritures manuelles inhabituelles

Signaux documentaires

- Documents manquants ou photocopiés
- Justificatifs modifiés ou raturés
- Approbations absentes ou imitées
- Incohérences de dates et de numéros
- Absence de piste d'audit

Signaux organisationnels

- Concentration des pouvoirs sur une personne
- Contrôles contournés « par exception »
- Forte rotation dans une fonction sensible
- Culture de la performance à tout prix
- Plaintes répétées de tiers

Prudence — un red flag est une invitation à investiguer, pas une accusation. Toute suite doit respecter la présomption d'innocence, la confidentialité et la procédure d'enquête.

Le contrôle le plus rentable

Le signalement révèle plus de fraudes que toute autre méthode. Encore faut-il que le canal existe, soit connu et inspire confiance.

43%

des fraudes découvertes par
signalement

52%

des signalements émanent des
employés

× 1/2

pertes réduites de moitié avec
une ligne active

Les conditions d'efficacité

- **Multi-canal** — web, téléphone, e-mail ; le web est désormais le canal préféré.
- **Confidentialité & anonymat** — possibilité de signaler sans révéler son identité.
- **Protection du lanceur d'alerte** — interdiction stricte de toute représaille.
- **Accessible aux tiers** — clients et fournisseurs sont à l'origine d'un tiers des signalements.
- **Traitement tracé** — accusé de réception, instruction indépendante, retour au lanceur.

Une ligne d'éthique qui n'est pas connue ou pas crédible ne sert à rien. La **communication régulière** et le traitement exemplaire des premiers signalements construisent la confiance qui alimente le dispositif.

Faire parler la donnée

L'analyse de données permet de tester 100 % des transactions, et non un échantillon. Elle révèle des schémas invisibles à l'œil humain.

Tests de règles & exceptions

Doublons de factures, paiements le week-end, fournisseurs partageant un RIB ou une adresse avec un salarié, montants juste sous les seuils.

Loi de Benford

L'analyse de la distribution des premiers chiffres détecte les jeux de données manipulés, où les chiffres ne suivent plus la fréquence naturelle attendue.

Détection d'anomalies & clustering

Les algorithmes isolent les comportements atypiques par rapport à un profil normal, sans règle prédéfinie — utile contre les schémas inconnus.

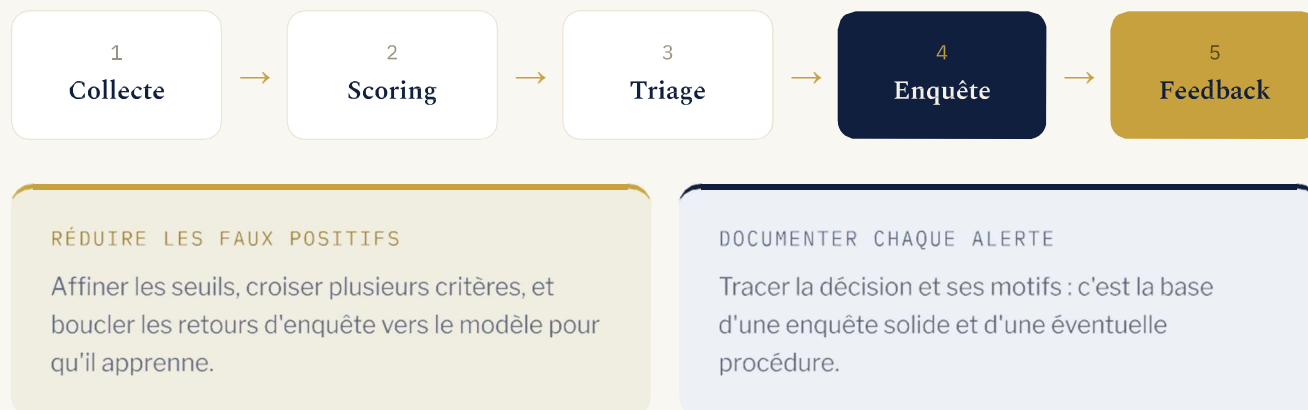
Scoring & apprentissage automatique

Un score de risque est attribué à chaque transaction en temps réel, priorisant les alertes les plus probables et réduisant les faux positifs au fil de l'apprentissage.

Réalité de terrain — dans de nombreuses organisations, la détection repose encore largement sur des processus manuels et des règles. Le passage à l'analyse continue est le principal gisement de progrès.

Maîtriser le flot d'alertes

Le défi n'est pas de générer des alertes, mais de les **traiter utilement**. Un système qui crie trop fort et trop souvent finit par être ignoré : c'est le piège du faux positif, qui peut atteindre des taux très élevés et éroder la confiance des équipes.



De l'audit ponctuel à la surveillance permanente

L'audit traditionnel regarde le passé par échantillon. L'**analyse continue** surveille l'intégralité des flux en quasi temps réel, rapprochant la détection du moment de la fraude — et réduisant d'autant la perte.

HIER

Audit par échantillon

Rétrospectif, partiel, annuel. Détecte tard, parfois jamais. La perte court pendant des mois.

DEMAIN

Surveillance continue

Exhaustif, temps réel, automatisé. Détecte tôt, alerte vite. La fenêtre de perte se referme.

Conditions de réussite

- **Qualité & accès aux données** — fondation indispensable de toute analyse fiable.
- **Compétences mixtes** — auditeurs et data analysts travaillant ensemble.
- **Gouvernance des modèles** — éviter les biais, documenter, auditer les algorithmes.
- **Respect de la vie privée** — proportionnalité et conformité à la protection des données.

CHAPITRE

08

Fraude télécoms & RAFM

Le cadre CFCA appliqué aux opérateurs : un secteur où la fraude se compte en dizaines de milliards.

Le RAFM, gardien des revenus de l'opérateur

Le RAFM réunit deux disciplines complémentaires : garantir que chaque service rendu est correctement facturé et encaissé, et empêcher l'usage frauduleux du réseau.

Revenue Assurance

Détecter les fuites de revenus : erreurs de taxation, écarts de médiation, services consommés mais non facturés, réconciliation entre réseaux et facturation.

Fraud Management

Détecter et bloquer l'usage frauduleux : abonnements frauduleux, contournement, partage de revenus internationaux, manipulation de comptes.

L'ampleur du phénomène (CFCA)

41,8 Md\$

pertes mondiales 2025

2,5%

des revenus du secteur

+3 Md\$

de pertes en deux ans

Source : CFCA Global Fraud Loss Survey. Un point particulièrement sensible pour les marchés émergents et africains, où le mobile concentre l'essentiel des usages.

Un catalogue qui évolue vite

IRSF

Partage de revenus internationaux — génération de trafic vers des numéros premium pour en partager les recettes. ~6,2 Md\$ de pertes en 2023.

Abonnement

Subscription fraud — souscription avec une identité volée ou sans intention de payer. Première source de pertes en valeur (~10 Md\$ cumulés).

SIM box

Contournement / bypass — réacheminement d'appels internationaux en appels locaux via des passerelles illégales, privant l'opérateur de ses revenus d'interconnexion.

Wangiri

Appels en absence — appels très courts incitant la victime à rappeler un numéro surtaxé. Variante « 2.0 » à grande échelle automatisée.

PBX / ATO

Piratage & prise de contrôle — intrusion dans un autocommutateur d'entreprise ou prise de contrôle de compte (SIM swap) pour générer du trafic frauduleux.

Spoofing

Usurpation & smishing — falsification du numéro appelant et SMS frauduleux, désormais première préoccupation des opérateurs, amplifiés par l'IA.

Le moteur de gestion de la fraude (FMS)

En télécoms, la donnée d'usage (CDR) est massive et continue. La détection repose sur l'analyse de ces tickets, idéalement en quasi temps réel pour stopper la fraude avant qu'elle ne se chiffre.

Analyse des CDR

Profilage des usages, destinations à haut risque, durées et volumes anormaux.

Contrôles de vitesse

Détection des pics soudains de trafic, de dépenses ou d'activation, signature des fraudes massives.

Seuils & règles

Plafonds de crédit, listes de numéros à risque, blocage automatique au-delà d'un seuil.

Modèles & collaboration

Apprentissage automatique et partage inter-opérateurs de listes de menaces (IRSF, numéros frauduleux).

LE DÉFI DES FAUX POSITIFS

Les systèmes à seuils génèrent souvent de nombreux faux positifs, qui dégradent l'expérience client et noient les vraies alertes. L'enjeu : combiner règles et modèles pour **bloquer la fraude sans pénaliser les abonnés légitimes**. Les petits opérateurs sur infrastructure ancienne restent les plus exposés.

Sept bonnes pratiques pour les opérateurs

1 **KYC robuste** à l'activation : vérification d'identité contre la fraude à l'abonnement.

2 **Surveillance temps réel** des CDR et des seuils de dépense.

3 **Réconciliation revenue assurance** de bout en bout réseau-facturation.

4 **Protection contre le SIM swap** et l'authentification renforcée.

5 **Collaboration inter-opérateurs** et partage de listes de menaces.

6 **Modernisation des réseaux** : la migration vers l'IP réduit les angles morts.

7 **Gouvernance RAFM dédiée** — une équipe rattachée au risque/conformité, des KPI suivis par la direction, et une veille permanente sur des fraudes qui se réinventent en continu.

Tendance — la fraude télécoms glisse de la technique pure vers la **manipulation de comptes et d'identité** : près de la moitié des principales méthodes relèvent désormais de ce registre. Le facteur humain redevient central.

CHAPITRE

09

Plan d'action & réponse à incident

Du programme anti-fraude à la gestion de crise : agir avant, pendant et après.

Lancer ou renforcer le dispositif

Jours 1–30 — Diagnostiquer

FFOUNDATIONS

Cartographier les risques de fraude, recenser les contrôles existants, évaluer la maturité, obtenir le parrainage de la direction et du comité d'audit.

Jours 31–60 — Outiller

QUICK WINS

Activer la ligne d'éthique, publier le code de conduite, combler les failles critiques (séparation des tâches, anti-BEC), lancer la sensibilisation.

Jours 61–90 — Pérenniser

ANCORAGE

Mettre en place les KRI et le reporting, démarrer l'analyse de données, formaliser le plan de réponse à incident, planifier la revue annuelle.

Principe directeur — mieux vaut un dispositif simple, appliqué et vivant qu'un programme sophistiqué resté sur le papier. La maturité se construit par itérations, pas d'un seul coup.

Les six temps de la réponse

1. Sécuriser & préserver

Stopper l'hémorragie, geler les accès et préserver les preuves (chaîne de garde) sans alerter prématurément le suspect.

2. Constituer la cellule

Réunir audit, juridique, RH, sécurité (et direction selon la gravité). Définir qui décide et qui communique.

3. Enquêter

Établir les faits avec méthode et impartialité : analyse documentaire et de données, entretiens, quantification du préjudice.

4. Décider des suites

Sanction disciplinaire, plainte pénale, action civile en recouvrement, déclarations réglementaires éventuelles.

5. Remédier

Corriger la faille de contrôle exploitée pour empêcher toute récurrence par le même vecteur.

6. Capitaliser

Retour d'expérience documenté, mise à jour de la cartographie et des KRI, communication interne mesurée.

Rigueur, impartialité, légalité

À faire

- ✓ Préserver les preuves et leur intégrité
- ✓ Documenter chaque étape et décision
- ✓ Respecter la confidentialité
- ✓ Présumer l'innocence jusqu'aux faits établis
- ✓ Associer le juridique très tôt
- ✓ Limiter le cercle des informés

À éviter

- × Confronter le suspect prématurément
- × Détruire ou altérer des preuves
- × Accuser sans éléments solides
- × Recourir à des moyens illégaux
- × Communiquer largement en interne
- × Promettre une issue avant l'enquête

LA PREUVE, NERF DE LA PROCÉDURE

Une preuve obtenue de façon irrégulière peut être écartée et fragiliser toute la procédure. La **chaîne de garde** — qui a eu accès à quoi, quand et comment — doit être tracée du premier instant. En cas de doute, faire intervenir des spécialistes en investigation et en preuve numérique.

Gérer la dimension réputationnelle

La fraude est aussi une crise de confiance. Une communication maîtrisée — interne comme externe — protège la réputation autant que les chiffres. Le silence total comme la sur-communication sont deux écueils.

Interne

Messages factuels et mesurés ; réaffirmer les valeurs et la fermeté de la réponse, sans nommer ni stigmatiser.

Régulateur

Respecter les obligations de déclaration (blanchiment, données, secteur régulé) dans les délais impartis.

Externe

Une voix unique, des faits vérifiés, un porte-parole identifié. Anticiper les questions plutôt que subir.

À préparer à froid — un plan de communication de crise rédigé *avant* l'incident fait gagner un temps décisif. On ne rédige pas une stratégie sous pression, le jour J.

Quatre niveaux de maturité anti-fraude

1

Réactif

On traite la fraude quand elle survient. Pas de cartographie, contrôles épars, dépendance au hasard.

2

Structuré

Politique, code de conduite et ligne d'éthique en place. Contrôles documentés, cartographie initiale.

3

Proactif

KRI suivis, analyse de données, revue régulière de la cartographie. La détection précède l'incident.

4

Optimisé

Surveillance continue, modèles prédictifs, culture d'intégrité ancrée. La maîtrise de la fraude devient un avantage.

Où en êtes-vous ? Situer honnêtement son niveau est le premier pas. L'objectif n'est pas d'atteindre le niveau 4 partout, mais d'aligner la maturité sur l'exposition réelle de chaque processus.

CHAPITRE

10

Boîte à outils

Check-lists prêtes à l'emploi, glossaire et références pour passer de la lecture à l'action.

Les fondamentaux à vérifier

PRÉVENIR

- ☐ Politique anti-fraude validée par la gouvernance
- ☐ Code de conduite signé par tous les collaborateurs
- ☐ Séparation des tâches sur les processus sensibles
- ☐ Due diligence KYC sur fournisseurs et partenaires
- ☐ Procédure anti-BEC (double canal + double validation)

DÉTECTER

- ☐ Ligne d'éthique active, connue et protégée
- ☐ Rapprochements indépendants et réguliers
- ☐ Cartographie des risques de fraude à jour
- ☐ KRI suivis et tableau de bord partagé
- ☐ Tests de données récurrents (doublons, anomalies)

RÉAGIR

- ☐ Plan de réponse à incident formalisé et testé
- ☐ Cellule de crise et porte-parole identifiés
- ☐ Politique de sanction homogène et appliquée

Ce que la gouvernance doit savoir

- 01 Connaissons-nous nos cinq principaux risques de fraude et leur niveau résiduel ?
- 02 La cartographie des risques de fraude a-t-elle été revue cette année ?
- 03 La ligne d'éthique fonctionne-t-elle ? Combien de signalements, et avec quel suivi ?
- 04 L'audit interne est-il indépendant et doté des moyens d'investiguer la fraude ?
- 05 Les contrôles clés sont-ils testés, ou seulement supposés en place ?
- 06 Qui pourrait contourner les contrôles, et qui contrôle les dirigeants ?
- 07 Sommes-nous protégés contre la fraude au virement et l'usurpation par IA ?
- 08 Disposons-nous d'un plan de réponse à incident, et a-t-il été testé ?
- 09 Le « ton donné par le sommet » est-il cohérent avec nos exigences éthiques ?
- 10 Notre niveau de maturité anti-fraude est-il aligné sur notre exposition réelle ?

La maîtrise de la fraude, un actif stratégique

Tout au long de ce guide, une idée revient : la fraude n'est ni une fatalité, ni un pur problème de contrôle. Elle naît de la rencontre entre une pression, une opportunité et une justification — et c'est sur l'**opportunité** que l'organisation garde la main.

Les chiffres de l'ACFE et de la CFCA le confirment : plus d'une fraude sur deux est rendue possible par une défaillance de contrôle, et la détection précoce — portée par le signalement bien plus que par l'audit — est le premier levier d'économie. Prévenir, détecter, réagir : les trois temps se renforcent mutuellement.

Construire ce dispositif n'exige pas des moyens démesurés. Il exige de la **méthode**, de la **constance** et un **engagement réel de la gouvernance**. Une politique claire, une ligne d'éthique vivante, une cartographie tenue à jour et une culture d'intégrité valent davantage que les outils les plus sophistiqués laissés sans pilotage.

L'organisation qui s'y engage ne se contente pas de réduire ses pertes : elle protège sa réputation, renforce la confiance de ses parties prenantes et se dote d'un avantage durable. C'est dans cet esprit que TRIUM Solutions & Consulting accompagne ses clients — pour que la maîtrise de la fraude devienne, chez eux aussi, un actif stratégique.

« La meilleure défense contre la fraude n'est pas un logiciel, c'est une organisation qui voit, qui dit et qui agit. »

Glossaire

ACFE

Association of Certified Fraud Examiners, référence mondiale de l'examen de fraude.

Appétence au risque

Niveau de risque résiduel qu'une organisation accepte de supporter.

BEC

Business Email Compromise — fraude au virement par usurpation d'e-mail.

CDR

Call Detail Record — ticket d'usage télécom analysé en RAFM.

CFCA

Communications Fraud Control Association, référence de la fraude télécoms.

COSO

Cadre de référence du contrôle interne en cinq composantes.

FMS

Fraud Management System — moteur de détection de la fraude télécom.

IIA

The Institute of Internal Auditors, référence de l'audit interne.

IRSF

International Revenue Share Fraud — fraude au partage de revenus internationaux.

KRI

Key Risk Indicator — indicateur clé de surveillance du risque.

KYC

Know Your Customer — vérification de l'identité d'un client ou tiers.

RAFM

Revenue Assurance & Fraud Management — maîtrise des revenus et fraudes télécoms.

Risque inhérent

Niveau de risque avant prise en compte des contrôles.

Risque résiduel

Niveau de risque subsistant après l'effet des contrôles.

SIM swap

Prise de contrôle d'un numéro mobile pour intercepter codes et accès.

Tip / signalement

Alerte d'un tiers ou collaborateur, première source de détection.

Triangle de la fraude

Modèle : pression, opportunité, rationalisation.

Wangiri

Fraude à l'appel en absence incitant à rappeler un numéro surtaxé.

Références & sources

Les statistiques de ce guide proviennent de sources publiques. Pour les chiffres détaillés, se référer aux publications originales des institutions citées.

ACFE — Occupational Fraud 2024: A Report to the Nations

Association of Certified Fraud Examiners. Étude mondiale sur 1 921 cas dans 138 pays — typologies, pertes médianes, méthodes de détection, profils. [acfe.com](https://www.acfe.com)

CFCA — Global Fraud Loss Survey (2023, 2025)

Communications Fraud Control Association. Estimation des pertes mondiales de fraude télécoms et typologies par montant. [cfca.org](https://www.cfca.org)

IIA — Cadre de référence international & modèle des trois lignes

The Institute of Internal Auditors. Normes professionnelles de l'audit interne et gouvernance du risque. [theiia.org](https://www.theiia.org)

COSO — Internal Control & Enterprise Risk Management Frameworks

Committee of Sponsoring Organizations. Référentiels du contrôle interne et du management des risques.

Les valeurs chiffrées sont des ordres de grandeur issus des éditions publiées des rapports cités, arrondies à des fins de lisibilité. Elles sont susceptibles d'évoluer ; consultez les éditions les plus récentes pour vos analyses opérationnelles.

Comprendre, cartographier, détecter, maîtriser.

Un guide pratique pour bâtir un dispositif anti-fraude robuste, fondé sur les référentiels de l'ACFE, de l'IIA et de la CFCA. Des définitions aux statistiques 2024-2026, des schémas aux check-lists, il s'adresse aux dirigeants, auditeurs internes,



TRIUM Solutions & Consulting SARL

Douala, Cameroun · RAFM Academy

contact@rafmacademy.com

+237 699949990 / +237 672157776

· www.rafmacademy.com