ifaci

institut français de l'audit et du contrôle internes

Cahier de la Recherche

La fraude

Comment mettre en place et renforcer un dispositif de lutte anti-fraude ?

Réalisé par une Unité de Recherche

L'IFACI est affilié à The Institute of Internal Auditors

Dans la même collection

- **La création de valeur par le contrôle interne**, Unité de Recherche IFACI *(septembre 2010)*
- **Pour un urbanisme du contrôle interne efficient - Prises de position du Groupe Professionnel Banque**, Groupe Professionnel « Banque » *(avril 2010)*
- **L'audit de la fraude dans le secteur bancaire et financier**, Groupe Professionnel « Banque » *(janvier 2010)*
- **Création et gestion d'une petite structure d'audit interne**, Unité de Recherche IFACI *(janvier 2009)*
- **Une démarche d'audit de plan de continuité d'activité**, Unité de Recherche IFACI *(juillet 2008)*
- **Guide d'audit du développement durable : comment auditer la stratégie et les pratiques de développement durable ?**, Unité de Recherche IFACI *(juin 2008)*
- **Contrôle interne et qualité : pour un management intégré de la performance**, Unité de Recherche IFACI *(mai 2008)*
- **Des clés pour la mise en œuvre du contrôle interne**, Unité de Recherche IFACI *(avril 2008)*
- **Evaluer et développer les compétences des collaborateurs**, Antenne régionale Aquitaine IFACI *(novembre 2007)*
- **Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement – 2ème Edition**, Groupe Professionnel «Banque » *(janvier 2007)*
- **La cartographie des risques**, Groupe Professionnel « Assurance » *(juillet 2006)*
- **L'audit interne et le management des collectivités territoriales**, Unité de Recherche IFACI *(mai 2006)*
- **Une démarche de management des connaissances dans une direction d'audit interne**, Unité de Recherche IFACI *(mai 2006)*
- **L'auto-évaluation du contrôle interne**, Unité de Recherche IFACI *(octobre 2005)*
- **Cartographie des Risques**, Groupe Professionnel « Immobilier Locatif » *(septembre 2005)*
- **Étude du processus de management et de cartographie des risques**, Groupe Professionnel « Industrie et commerce » *(janvier 2004)*
- **Pour un bon audit du dispositif de lutte contre le blanchiment des capitaux**, Groupe Professionnel « Banque » *(février 2004)*
- **L'efficacité des Comités d'audit – Les meilleures pratiques**, PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Gouvernement d'entreprise et Conseil d'administration**, PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*

Pour plus d'informations : www.ifaci.com

© IFACI – Paris – décembre 2010

ISBN : 978-2-915042-219-4 – ISSN : 1778-7327

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

© IFACI

Remerciements

L'IFACI tient tout particulièrement à remercier les membres de l'Unité de Recherche qui, sous la responsabilité de **Jean-François SAUTIN**, *Senior Vice Président Group Audit, LAFARGE*, ont conçu et rédigé ce cahier :

- **Conception et rédaction :**
  Youssef ATMANE, *Consultant prévention et maîtrise des risques, CNAMTS ;*
  Patrick CALIFE, *Responsable du contrôle périodique, UNION FINANCIÈRE DE FRANCE BANQUE ;*
  Pierre DROUARD, *Pilote du Système Qualité, RENAULT ;*
  Stanislas FEIXAS, *Manager, DELOITTE ;*
  Olivier FONTANIE, *Directeur de mission – audit interne, EDF ;*
  Marc FOURRIER, *Directeur de la conformité, ALLIANZ FRANCE ;*
  Philippe GREAT, *Responsable sécurité financière, GROUPAMA BANQUE ;*
  Marc PELIEL, *Directeur de missions, LAFARGE ;*
  Jacques PELON, *Chargé de mission – contrôle interne, GROUPAMA SA ;*
  Catherine VAN DER LINDEN, *Directeur sectoriel de l'Audit Groupe, TOTAL.*

- **Comité éditorial :**
  Bernard DECOEUR, *Chargé de mission, Direction Audit et Risques, Service du contrôle interne, GDF-Suez ;*
  Béatrice KI-ZERBO, *Directeur de la Recherche, IFACI ;*
  Emmanuel PASCAL, *Audit Manager, BRAKE GROUP ;*
  Jean-François SAUTIN, *Senior Vice-President Group Audit, LAFARGE.*

- **Conception :**
  Laurent ARNAUDO, *Vice-President Corporate Audit, SODEXO ;*
  Marie-Estelle BAUFUME, *Responsable risques, procédures et méthodologie, VIVENDI ;*
  Mona GREGORI, *Manager, DELOITTE ;*
  Hugh PENRI-WILLIAMS, *Administrateur, ACFE Chapitre France.*

Ces travaux s'insèrent dans le cadre du **Groupe Professionnel « contrôle interne » de l'IFACI** qui est actuellement présidé par **Laurent ARNAUDO**, *Vice-President Corporate Audit, SODEXO.*

- **Mise en forme :**
  Julie FERRE, *Chargée de projets de la recherche, IFACI*

Par ailleurs, l'IFACI remercie **Jean-Victor PREVOST**, *Associé, Taj - Société d'avocats Membre de Deloitte Touche Tohmatsu*, pour les points de vigilance portant sur certains aspects juridiques de la fraude.

Louis VAURS, *Délégué Général, IFACI*

© IFACI

Sommaire

Synthèse **7**

Partie 1 - De quoi parle-t-on ? **9**
1.1 - Définition de la fraude 11
1.2 - Catégories / Typologies de risques de fraudes 14
1.3 - Les facteurs déclenchant : le triangle de la fraude 17

Partie 2 - Etat des lieux préalable au calibrage du dispositif anti-fraude **19**
2.1 - Un cadre cohérent et explicite 21
2.2 - Des dispositions concrètes pour l'action 21
2.3 - Un environnement général de contrôle mature 21
2.4 - Le contrôle des processus métiers 22

Partie 3 - Construction et pilotage du dispositif anti-fraude **23**
3.1 - Une politique anti fraude est définie au plus haut niveau 25
3.2 - La mise en œuvre de la politique mobilise différents acteurs et s'appuie sur des outils complémentaires 25
3.3 - Un pilotage adapté à chaque composante du programme 27
3.3.1 - Prévention : des hommes et des risques 28
3.3.2 - Détection : contrôler pour stopper ou découvrir vite 30
3.3.3 - Investigation et traitement : établir les éléments factuels et sanctionner les auteurs 33
3.3.4 - Correction : éviter la répétition 34

Partie 4 - Réagir face à un soupçon de fraude ou traiter un cas avéré **35**
4.1 - Pré-requis pour mener une investigation 37
4.1.1 - Disposer de modalités de remontée des soupçons claires et connues 37
4.1.2 - Disposer d'une organisation de gestion de crise connue et mobilisable dans les délais requis pour traiter les incidents 39
4.2 - Phase de découverte d'une anomalie 41
4.2.1 - Principales sources d'information 41
4.2.2 - Première évaluation des risques 42
4.2.3 - Quelques autres précautions à prendre 42
4.2.4 - Premiers échanges avec la direction générale 43
4.3 - Phase de pré-investigation 44
4.3.1 - Exemple de feuille d'analyse du soupçon de fraude en phase de pré-investigation 44
4.3.2 - Représentation conceptuelle du schéma de fraude : le logigramme 45
4.3.3 - Approche intuitive 45
4.3.4 - La phase de remontée de l'information 46
4.4 - Evaluation des enjeux et calibrage des moyens 47
4.4.1 - Précautions en termes de confidentialité 47
4.4.2 - Les ressources nécessaires pour conduire les investigations 48
4.4.3 - La nature et le niveau de reporting qui devront accompagner l'avancement de l'enquête 49
4.5 - Mesures conservatoires 50
4.6 - Phase d'investigation 51
4.6.1 - Objectifs de la phase d'investigation 51
4.6.2 - Gestion du temps 52

© IFACI

4.6.3 - Intervenants 52
4.6.4 - Travaux à réaliser 53
4.6.5 - Recherche de document ou de données 54
4.6.6 - Entretiens 54
4.6.7 - Précautions à prendre 55
4.6.8 - Analyse comportementale 56
4.6.9 - Investigation judiciaire 57
4.7 - Conclusion 59
4.7.1 - Comment préparer la conclusion ? 59
4.7.2 - Prise de décision 59
4.7.3 - Agir en conséquence 60
4.7.4 - Gérer les conséquences 61

Partie 5 - Un outil de prévention et d'anticipation : la cartographie des risques de fraude **63**
5.1 - Objectifs de la cartographie des risques de fraude 65
5.2 - Les étapes de l'élaboration de la cartographie des risques de fraude 66
5.2.1 - Définir une approche 66
5.2.2 - Identifier les risques majeurs inhérents 68
5.2.3 - Identifier les faits générateurs et les conséquences des risques 70
5.2.4 - Déterminer le niveau des risques inhérents de fraude et le niveau des risques nets perçus 71
5.2.5 - Evaluation indépendante du niveau d'exposition 73
5.3 - Synthèse et démarche de suivi 74
5.3.1 - Synthèse des travaux 74
5.3.2 - Démarche de suivi de la cartographie des risques 75

Partie 6 - Capitaliser l'expérience à partir des cas avérés **77**

ANNEXES **83**
Annexe 1 : Grille de diagnostic préalable : Etat des lieux du dispositif anti-fraude 84
Annexe 2 : Illustration de l'arborescence des types de fraude 95
Annexe 3 : Exemple de politique anti-fraude 100
Annexe 4 : Exemple de typologie de risques 105
Annexe 5 : Fiches 108
Echange frauduleux de composants informatiques 109
Utilisation frauduleuse de moyens de paiement 112
Détournement de fonds par un collaborateur 115
Détournement physique de matériel 119
E-commerce 122
Utilisation frauduleuse des moyens de l'entreprise à des fins personnelles 125
Prestations factices facturées à l'entreprise (1) 128
Prestations factices facturées à l'entreprise (2) 131
Fausses pièces justificatives – Dossier de crédit 134
Falsification de pièces justificatives d'un dossier entrée en relation 138

BIBLIOGRAPHIE **141**

© IFACI

© IFACI

Synthèse

Le Cahier de la Recherche « Comment mettre en place et renforcer le dispositif de lutte contre la fraude » s'inscrit dans la volonté d'offrir aux **opérationnels** et aux responsables de **structures d'audit ou de contrôle interne** une réflexion pédagogique et un guide pratique pour la mise en œuvre effective d'une organisation et de moyens de prévention et de traitement du risque de fraude.
Il s'agira pour eux, dans un premier temps, de pouvoir évaluer le niveau de maturité et d'expérience de leur organisation par rapport aux situations de fraude auxquelles l'expérience commune montre que nul n'échappe. Ils pourront ensuite réfléchir à la façon la mieux adaptée à leur propre organisation, dans son environnement particulier, **pour structurer ou faire progresser** un dispositif spécifique de prévention et de traitement des situations de fraude ou de suspicion de fraude.

Les débats de l'unité de recherche ont renforcé auprès de ses participants la conviction que tous les acteurs de l'organisation ont un rôle à jouer pour réduire le risque de fraude.

La confiance entre les participants d'un même projet d'organisation est un ingrédient essentiel de sa réussite, et souvent, aborder au sein d'une entité le thème de la fraude - en raison du caractère dissimulé des actes qui la sous-tendent - tend à être perçu comme contraire à cet esprit d'organisation. Un des éléments de maturité observable dans une organisation sera certainement la façon dont le sujet est abordé au travers de la communication interne, **sans pudeur excessive ni curiosité malsaine, et dans le respect des personnes.** Construire une communication interne adaptée est sans doute un des éléments du dispositif de prévention de la fraude.
Les dirigeants jouent bien sûr un rôle clé pour donner le ton, et permettre de transformer le caractère « déplaisant » du sujet fraude en élément de clarté et de motivation au sein de l'organisation. En effet, de nombreuses études confirment que les employés qui respectent les règles du jeu sont sensibles à une approche proactive au sein de leur organisation pour prévenir le risque de fraude (sentiment de qualité) et sanctionner les dérapages (sentiment de justice).

Le thème de la fraude a ceci de particulier qu'il est au carrefour de préoccupations éthiques et de processus généralement explicites de contrôle interne. Il est clair qu'une approche trop exclusivement fondée sur les processus ou la technologie ne suffira pas, comme le démontrent quotidiennement de nombreux faits divers plus ou moins sensationnels ou sordides. A l'inverse, une approche trop fondée sur la sociologie ou la psychologie du fraudeur potentiel manquera son objectif, faute de moyens de contrôle précis et efficaces. Il s'agira donc, dans ce cahier de la recherche, d'éviter deux pièges : l'un qui consisterait à n'offrir qu'un discours trop appuyé sur la dimension éthique, et l'autre qui serait de refaire implicitement un traité de contrôle interne.

- Une <u>première partie</u> traitera des définitions : **« La Fraude : de quoi parle-t-on ? »**. Il s'agit dans cette section de donner un aperçu général du thème et de sa spécificité par rapport aux autres préoccupations de l'audit ou du contrôle interne.

© IFACI

- La seconde partie brossera le tableau des **pré-requis indispensables** pour qu'un dispositif de prévention et de traitement des cas de fraude soit efficace. Ainsi, un état des lieux de la maturité de l'organisation apparaît aux participants de ce cahier de la recherche comme une étape importante avant le calibrage du dispositif à mettre en œuvre.

- La troisième partie traitera de la **construction et du pilotage du dispositif anti-fraude**. Parmi les questions clés que nous nous poserons, citons :
  - comment faire travailler des industriels sur le sujet fraude lorsque ce n'est pas leur préoccupation première ?
  - comment exploiter au mieux une base d'incidents ?
  - quel rôle pour les différents acteurs impliqués dans le dispositif ?
  - quelles précautions prendre pour respecter les lois et les personnes ?

- Une quatrième partie illustrera ces principes de pilotage lorsqu'une **fraude est soupçonnée ou avérée.**

- Une cinquième partie sera consacrée à l'anticipation et la prévention par le déploiement et l'animation d'une **cartographie des risques de fraude.** Une telle cartographie est un vecteur potentiel pour une prise de conscience largement partagée au sein de l'organisation.

- Enfin, ce cahier de la recherche proposera – de façon bien sûr non exhaustive, tant les fraudeurs savent être créatifs - des **fiches pratiques de maîtrise des risques de fraude** et de mise en œuvre de contrôles pratiques.

Nous espérons que ce cahier de la recherche contribuera à démythifier ce qui est encore trop souvent un tabou et permettra à des équipes motivées de poser des actes concrets, pragmatiques et adaptés à la culture et maturité de leur organisation pour y prévenir le risque de fraude.

L'objet de cette publication n'étant pas de traiter de manière exhaustive la dimension juridique de la fraude, nous invitons les lecteurs à prendre toutes les précautions et avis d'experts nécessaires à une prise en compte appropriée de cet aspect selon le contexte (étape du dispositif, type de fraude, réglementations locales, etc.).

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Partie 1

De quoi parle-t-on ?

La fraude est un terme générique qui recouvre des situations et des actions très diverses. Il est donc parfois difficile d'en définir les contours. De plus, outre les différents délits et malversations sous-jacents, la fraude renvoie à des notions d'éthique dont la perception est souvent variable d'une culture ou d'une organisation à une autre. Cette dimension éthique ne sera pas développée dans cette publication.

Cette première partie du cahier de la recherche propose une définition de la fraude. Il ne s'agit pas d'un simple exercice sémantique, puisque la définition de la fraude constitue le fondement de toute politique de lutte anti-fraude.
Plus concrètement, la typologie et le rappel des faits générateurs décrits dans le triangle de la fraude (Cf. partie 1.3 p. 17) rendent compte de l'amplitude des faits visés et de leur caractère multiforme.

© IFACI

© IFACI

1.1. Définition de la fraude

Le groupe de travail propose une définition de la fraude issue de l'analyse des positions des organisations professionnelles (IIA, ACFE) et des notions utilisées dans les organisations qui ont contribué à l'unité de recherche.

*« La fraude consiste à **tromper délibérément** autrui pour obtenir un **bénéfice illégitime**, ou pour contourner des obligations légales ou des règles de l'organisation. Un comportement frauduleux suppose donc un **élément factuel** et **intentionnel** ainsi qu'un procédé de dissimulation de l'agissement non autorisé. »*

Les éléments clés de cette définition sont commentés dans le tableau ci-après :

Elément	Remarques	Exemples
Délibéré/ Intentionnel	**Ce n'est pas une erreur.** Le fraudeur commet une action dont il connait le caractère non autorisé. La fraude peut être une action ou une omission.	• Utilisation du profil d'un autre utilisateur pour réaliser des transactions frauduleuses dans le système d'information. • Altération intentionnelle de données dans les systèmes d'information permettant de réaliser un détournement d'actifs. A contrario, des modifications de données commises par erreur ne sont pas des fraudes. • Omission intentionnelle d'une information significative dans les publications (financières ou opérationnelles) internes ou externes. A contrario, le *reporting* erroné du fait d'une faiblesse dans le processus d'élaboration ou de contrôle n'est pas une fraude. • Absence de contrôle des transactions des collaborateurs pour améliorer artificiellement les résultats de leur département. • A contrario, une absence de contrôle de sorties de stocks par insuffisance de moyens de contrôle ou faiblesse d'organisation n'est pas une fraude.

© IFACI

Elément	Remarques	Exemples
Illégitime	La fraude **ne peut être réduite à une définition légale voire pénale** et aux actes qui sont en infraction avec des dispositions législatives ou règlementaires. Certaines fraudes sont liées à un contournement de règles internes ou de principes éthiques établis par l'organisation. Elles n'ont pas forcément une conséquence pénale.	• Non respect du code de conduite de l'organisation. • Falsification de documents ou de données. • Dépassement délibéré des limites de transactions ou de positions dans les activités commerciales ou de *trading*.
Bénéfice recherché	Le **mobile de la fraude n'est pas exclusivement un gain matériel**.	• Appropriation d'actifs, gains financiers, avantages financiers ou en nature pour soi-même ou pour une personne de son entourage. • D'autres types de bénéfices peuvent être recherchés : - Volonté de reconnaissance. - Volonté de préserver une réputation pour soi-même ou son entité. - Esprit « joueur » du fraudeur qui jouit du plaisir de ne pas être pris « la main dans le sac ». - Impression d'agir dans l'intérêt de l'organisation (corruption pour l'obtention ou le renouvellement de contrats, ententes anticoncurrentielles pour préserver une part de marché, fraudes fiscales, falsifications de documents comptables, etc.).
Factuel	La fraude se matérialise par des comportements et des actes. Ces éléments objectifs permettent d'apprécier l'impact de la fraude.	• Vol de matière première.

© IFACI

Elément	Remarques	Exemples
Dissimulation	Cet élément est un corollaire du caractère illégitime de la fraude. Il justifie les complicités éventuelles.	• Faux et usage de faux. • Ecritures comptables permettant de dissimuler des mouvements de trésorerie frauduleux. • Falsification de données de suivi de réceptions / expéditions de biens afin de dissimuler des vols de produits dans les sites de stockage en collusion avec d'autres employés.
Parties prenantes	La fraude peut être le fait d'une personne ou d'une organisation, interne ou externe à l'organisation. La distinction entre fraude interne et fraude externe à l'organisation est utile pour la définition des modalités de prévention et de détection. Cependant, cette distinction n'est pas strictement discriminante en matière de définition.	• Vols d'actifs venant de tiers à l'organisation sans complicité interne. • Détournements de fonds réalisés par un collaborateur dans une organisation n'assurant pas une séparation des tâches suffisante. • Vols de produits de l'organisation par des tiers aidés par une complicité interne facilitant les accès ou/et dissimulant les éléments de preuves. • Agissement de collaborateurs sans complicité de tiers externes à l'organisation. • Actions de tiers. • Collusion / complicité entre collaborateurs et tiers.

- La fraude peut être le fait d'une personne ou d'une organisation, interne ou externe à l'organisation.
- Le mobile de la fraude peut être matériel (appropriation, gains ou économies, avantages) aussi bien que moral (sentiment d'obligation, volonté d'être reconnu ou de préserver une réputation) pour le fraudeur ou pour un tiers.
- La fraude peut être une action ou une omission.
- La fraude crée un préjudice financier, matériel, moral ou d'image à l'organisation ou à ses clients, partenaires ou autres interlocuteurs.

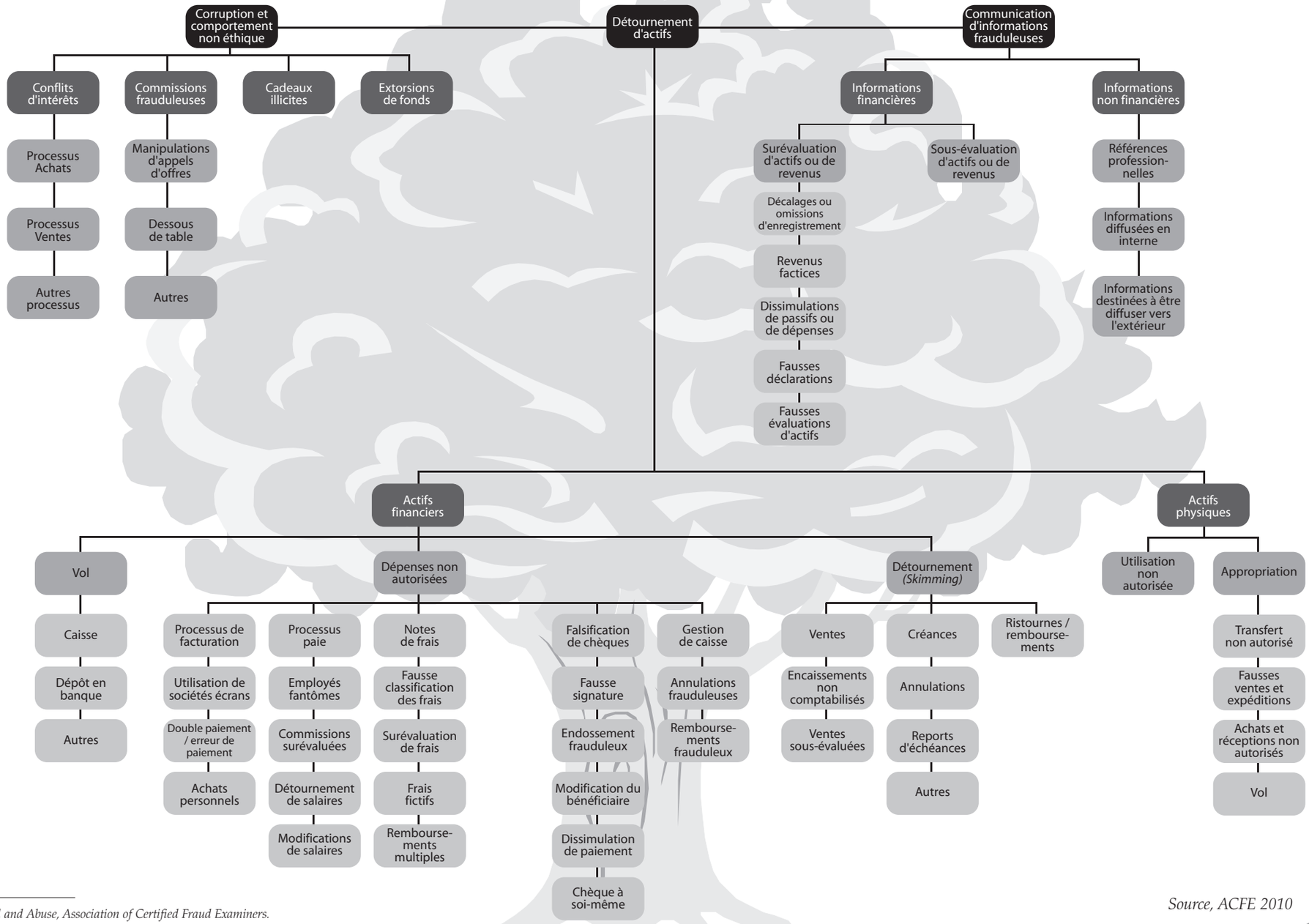
© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

1.2. Catégories / Typologies de risques de fraudes

Il est concrètement utile de catégoriser les fraudes selon différentes typologies qui, selon les activités de chaque organisation, vont être d'enjeux plus ou moins significatifs.

Cette catégorisation n'est pas encadrée au niveau légal ou règlementaire. L'unité de recherche propose une traduction de la classification diffusée par l'ACFE *(Association of Certified Fraud Examiners)*[1].



Source, ACFE 2010

[1] *2010 Report to the nations on occupational Fraud and Abuse, Association of Certified Fraud Examiners.*

© IFACI

© IFACI

- La **corruption** peut être passive ou active. Elle peut concerner différentes parties prenantes : des salariés, des fournisseurs, des clients, des administrateurs, des partenaires, des intermédiaires ou des agents publics.

- Il n'est pas toujours possible de prévenir les situations de **conflit d'intérêt**. Elles doivent être déclarées. Ce n'est pas la possibilité de conflit d'intérêt en elle-même qui est problématique, c'est son usage à des fins de favoritisme ou de népotisme qui est frauduleux.

- Il existe d'**autres situations de conflit d'intérêt** que celles qui concernent les relations vendeurs/acheteurs. Citons, par exemple, les ententes anticoncurrentielles ou les délits d'initiés (utilisation de la connaissance d'informations confidentielles dans le cadre de transactions sur des valeurs mobilières).

- La **falsification des données** peut être opérée lors de leur élaboration ou au cours de leur intégration dans la communication interne ou externe.

- La falsification des **données financières** peut affecter la qualité des états financiers, des déclarations fiscales, etc.

- La falsification des **données non financières** peut affecter les choix opérationnels internes, la qualité du suivi de performance des activités, voire les états financiers.

- Avec le développement des nouvelles technologies, les détournements d'actifs concernent également les **actifs incorporels et le patrimoine informationnel** de l'organisation.

Vous retrouverez des illustrations de la typologie fraude en annexe 2, p. 95.

D'autres exemples sur le site de la Gendarmerie Royale canadienne : http://www.grc-rcmp.gc.ca/scams-fraudes/index-fra.htm

Cette typologie est conçue comme un outil pour structurer la recherche des différents cas de fraude. Néanmoins, comme elle s'intéresse aux conséquences de la fraude, un même cas peut être répertorié à différents niveaux. Par exemple, la manipulation du résultat opérationnel par un reclassement intentionnel de données est une **falsification des états financiers**. Mais, ce type de manipulation peut également engendrer une majoration frauduleuse du bonus et donc un **détournement d'actif financier**.

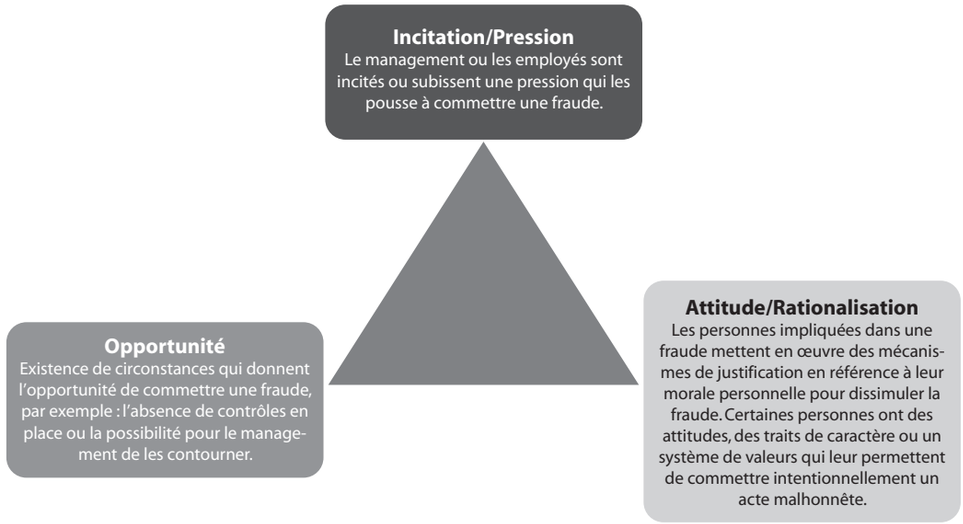
Pour plus d'efficacité, l'utilisation de cette typologie peut être croisée avec une approche par processus métiers ou selon la nature des faits générateurs (motivation-pression/ opportunité/ rationalisation des actes) présentés dans le paragraphe suivant.

© IFACI

1.3. Les facteurs déclenchant : le triangle de la fraude

Des données sur le profil type des fraudeurs sont régulièrement publiées dans les enquêtes sur la fraude. Ces statistiques masquent une réalité très diversifiée qui montre que le risque de fraude augmente quand certaines conditions individuelles ou structurelles sont réunies. Ces conditions peuvent être réunies en 3 grandes catégories illustrées par le fameux « triangle de la fraude ».

LE TRIANGLE DE LA FRAUDE



Opportunité	Incitation/Pression	Attitude/Rationalisation
• Failles du dispositif de contrôle interne (absence de contrôles, inefficacité des contrôles en place, possibilité de contourner les contrôles, erreurs non corrigées, absence de sanctions, etc.). • Système de gouvernance déséquilibré (absence de procédures/de contrôles compensatoires, gouvernance	➢ Indicateurs de performance trop exigeants. ➢ Système de rémunération. ➢ Besoin de reconnaissance. ➢ Contexte économique défavorable (compétition accrue, baisse des marges, faillites, besoin de financement, etc.).	o Rationaliser l'acte frauduleux comme étant un dû par rapport à ses valeurs et à sa propre éthique. o Autojustification fondée sur des arguments tels que : - une promotion manquée ; - une prime non accordée ; - « Tout le monde fait la même chose »…

© IFACI

Opportunité	Incitation/Pression	Attitude/Rationalisation
fondée sur la personnalité du manager). • Changement organisationnel et/ou de système d'information (transactions complexes, acquisitions, fort *turn over* des dirigeants, etc.). • Situations de position dominante vis-à-vis de clients ou de fournisseurs.	➢ Changements dans l'environnement ou dans l'organisation (évolutions technologiques, obsolescence des produits, nouvelles contraintes réglementaires, etc.). ➢ Incitations externes (corruption passive). ➢ Difficultés financières du fraudeur potentiel (dettes, jeu, projet, etc.).	o Cette autojustification du passage à l'acte sera d'autant plus aisée que l'environnement éthique ne favorise pas un cadre de bonne conduite.

L'intentionnalité étant une des caractéristiques de la fraude, il est important et utile de connaître les conditions propices au « passage à l'acte ». Leur connaissance est notamment utile pour des actions de sensibilisation ciblées et pour détecter des symptômes de fraude (cf. Partie 3, p. 23 et Partie 6, p. 77).
Ces conditions évoluent avec :

- la situation des personnes et des organisations ;
- les risques (par exemple, modes opératoires plus technologiques de certaines actions frauduleuses ou impact financier modifié du fait d'importantes augmentations de la valeur vénale de certains biens ou services) ;
- les contraintes légales, règlementaires ou opérationnelles affectant les activités.

En conclusion, les retours d'expérience en matière de sécurité industrielle peuvent servir de leçons. Ils montrent que dans un environnement qui peut paraître sécurisé, une catastrophe peut se produire à la suite de dérives successives. Il faut donc savoir rester vigilant par rapport aux signaux qui, même s'ils paraissent faibles, peuvent dégénérer et avoir des répercussions majeures. Par ailleurs, dans le secteur industriel, l'ensemble des collaborateurs a intégré le fait que chacun est responsable de la sécurité du site. Ils s'investissent donc dans cette démarche collective et développent une sensibilité aux signaux d'alerte.

La fraude touche toutes les dimensions de l'organisation. C'est une problématique très transversale, dont la maîtrise nécessite un double arsenal de méthodes (par exemple, la cartographie des risques de fraude, la gestion des soupçons, l'analyse des cas avérés, etc.) et d'attitudes (l'exemplarité selon le principe du *Tone at the Top*[1], la stratégie de pilotage, etc.) dont certaines sont détaillées dans la suite du cahier et récapitulées dans la partie 2, p. 19.

[1] *« How the management can prevent fraud in the workplace » presented by the Association of Certified Fraud Examiners (ACFE).*

© IFACI

Partie 2

Etat des lieux préalable au calibrage du dispositif anti-fraude

L'unité de recherche a recensé les éléments clés pour un état des lieux de l'organisation avant de s'engager dans l'action. En effet, en amont de la construction du dispositif, il est indispensable d'appréhender le niveau de maturité de son organisation pour trouver les angles de développement les mieux adaptés au contexte.
Quatre conditions de réussite incontournable sont rappelées ci-après.

© IFACI

© IFACI

2.1- Un cadre cohérent et explicite

L'encadrement du dispositif de lutte anti-fraude doit :

- reposer sur l'appui et l'impulsion des plus hautes instances de gouvernance et opérationnelles (PDG, Président, direction générale, conseil d'administration et, s'il existe, son Comité ad hoc) ;
- être fondé sur des valeurs reconnues et portées au sein de l'organisation (ou du groupe) qui ne laissent aucune ambiguïté sur l'éthique et son respect ;
- être caractérisé par une synergie entre les fonctions opérationnelles, contrôle interne, audit, risques, éthique et conformité pour renforcer le dispositif de prévention, de détection et de traitement des fraudes ;
- avoir fait l'objet d'échanges et de comparaisons (au moyen de démarches de *benchmarking* soigneusement préparées avec des organisations comparables (secteur d'activités, taille, organisation, etc.)).

2.2- Des dispositions concrètes pour l'action

telles que la diffusion de guides pratiques, les formations, les recommandations d'audit interne :

- donnent des points de repère, en précisant la signification de certains mots tels que « fraude », « corruption », « conflit d'intérêts », etc.
- déclinent le cadre de cohérence au sein des différents métiers et des différentes zones géographiques d'implantation de l'organisation (ou du groupe) ;
- présentent quelques mises en situation avec des éléments de réponse (ex. conflits d'intérêts, cadeaux, etc.).

2.3- Un environnement général de contrôle mature

Cet environnement de contrôle repose notamment, pour chaque processus clés de l'organisation, sur :

- des décisions d'organisations diffusées et connues ;
- des délégations de pouvoirs et des habilitations informatiques organisées et cohérentes (séparation des tâches incompatibles, habilitations informatiques reflétant les délégations de pouvoirs) ;
- un dispositif de pilotage pertinent nécessitant principalement : un responsable, un reporting organisé et une instance en charge d'examiner les situations jugées critiques, des *benchmarks* ;
- un traitement de la fraude conforme avec le cadre de cohérence défini par l'organisation (ou le Groupe) ;
- une analyse des défaillances de contrôle interne dans le cas de fraudes conduisant, si nécessaire, à modifier les organisations et/ou les contrôles ;

© IFACI

- une implication managériale, à tous les niveaux de l'organisation (ou du groupe), dans la prévention des fraudes pouvant s'exprimer dans une attestation (ex : déclaration de tous les cas de fraudes).

2.4- Le contrôle des processus métiers

L'efficacité du dispositif repose sur :

- la sélection des contrôles en place (ou à créer) qui participent à la prévention de la fraude dans les domaines touchant notamment à l'organisation (délégations de pouvoirs, habilitations informatiques, etc.), aux ventes, aux achats de toutes natures (produits finis, matières, prestations), aux frais de personnel, aux investissements ainsi qu'aux opérations comptables associées ;
- la mise en œuvre de ces contrôles en priorité dans les entités jugées à risques en prenant en compte le facteur pays et/ou activité ;
- le *reporting* des résultats des contrôles ;
- l'exploitation par le management des résultats.

Par ailleurs, l'unité de recherche vous propose une grille de diagnostic en annexe (cf. Annexe 1, p. 84). Cet outil facilitera :

- la priorisation des actions à mener ;
- l'identification des forces et des faiblesses de l'environnement général.

Cette grille ne vise pas l'exhaustivité. Vous pourrez donc compléter et adapter les éléments proposés en fonction de votre organisation.
Pour être plus opérationnel et pour hiérarchiser les actions à mettre en œuvre, les éléments de diagnostic ont été classés selon leur niveau de criticité. Votre jugement professionnel vous orientera dans le choix des éléments les plus pertinents dans votre contexte.

© IFACI

Partie 3

Construction et pilotage du dispositif anti-fraude

La fraude repose sur l'intention de tromper et la dissimulation, ce qui la rend potentiellement plus dangereuse que de simples erreurs, d'autant plus que le fraudeur est a priori tenté de pérenniser la fraude. Nombre de fraudes sont commises par une exploitation opportuniste et volontaire de faiblesses ou d'éléments de contexte techniques, organisationnels voire culturels. Le dispositif anti-fraude doit donc s'inscrire dans un cadre global de sensibilisation et de contrôle interne qui limite les faiblesses du système de gestion. Ce cadre devra prendre en compte la dimension éthique des activités définie au plus haut niveau de l'organisation.
Le dispositif à construire et ces modalités de pilotage dépendent de l'état des lieux en matière de contrôle interne et de lutte contre la fraude (cf. Partie 2, p. 19). Les expériences partagées au sein de cette unité de recherche font ressortir des constantes :

- Une réflexion **pluridisciplinaire** permettant :
  - d'établir un diagnostic préalable au déploiement de la politique ;
  - de recueillir les éléments d'aide à la décision pour le lancement du dispositif (Comment définir la fraude ? Comment la gère-t-on ? Quelles sont les composantes du dispositif ? Quels liens avec les démarches voisines (éthique, contrôle interne, risques) ? Que faire en situation de crise ?, etc.) ;
  - de mobiliser les décideurs pour un lancement effectif de la démarche ;
  - d'assurer le « maintien en condition opérationnel » du dispositif ou le passage de relais à une entité ad hoc « anti-fraude ».
- La clé du succès réside dans l'orientation donnée par les **organes dirigeants** et leurs implications dans le suivi du dispositif. Il convient de dépasser le simple affichage de bonnes pratiques pour un engagement réel. Plus qu'ailleurs, il ne faut pas donner l'impression qu'il peut y avoir des demi-mesures.
- La première ligne de défense, sans laquelle la démarche n'aboutira pas, est constituée par les opérationnels. Il convient donc de mobiliser tous les instruments de gestion de l'organisation pour positionner la lutte contre la fraude **au cœur des activités**.
- La **culture d'entreprise** (notamment le style de management et la relation Groupe/entités, etc.), la culture des métiers, le climat économique et social sont à prendre en considération pour construire un dispositif adapté et le faire vivre.

© IFACI

© IFACI

3.1- Une politique anti fraude est définie au plus haut niveau

Il est indispensable que le pilotage du dispositif s'inscrive dans le cadre d'une politique préparée par une cellule de cadrage et d'appui, adoptée au plus haut niveau de l'organisation et déclinée dans toutes les entités, les modalités de diffusion pouvant être annexées ou non au règlement intérieur (cf. annexe 3, p. 100). Son contenu synthétique comprend a minima les points suivants :

- définition de la fraude ;
- conséquences pour l'organisation, les tiers, les employés ;
- rappel des dispositions du règlement intérieur et du code de déontologie ;
- affirmation de la position de l'organisation (par exemple, « tolérance zéro ») ;
- traduction de la position en « promesses » d'actions : prévention, contrôle, sanction, poursuites, etc.

Pour être effective, cette politique devra être largement diffusée, accessible à tous et suivie d'effets.

Le pilotage du dispositif fait l'objet d'un cadrage proactif et pluridisciplinaire, pour :

- avoir un regard croisé intégrant les problématiques métiers, de contrôle interne et le facteur humain ;
- identifier les points de vigilance à l'égard de la fraude. Par exemple, les pressions sur l'organisation, ses dirigeants, ses employés, ses fournisseurs et ses prestataires peuvent être non négligeables et être une source de tentation pour commettre un acte frauduleux, soit isolé, soit en collusion interne ou interne/externe ;
- susciter la prise de conscience sur les risques de fraude et leurs conséquences (cf. Partie 5, p. 63) ;
- faire la part entre le cadrage global et les recadrages nécessaires au cas par cas.

3.2- La mise en œuvre de la politique mobilise différents acteurs et s'appuie sur des outils complémentaires

La mise en œuvre d'un programme anti-fraude s'inscrit dans l'environnement de contrôle interne. Elle s'appuie, tant que faire se peut, sur l'organisation existante. Toute mise en œuvre d'une politique requiert une spécification des rôles et des responsabilités, une classification des interactions entre les différents acteurs ainsi que les moyens d'évaluer les résultats attendus : la politique de lutte contre la fraude n'y déroge pas.

© IFACI

Exemples d'acteurs et d'outils de mise en œuvre de la politique anti-fraude (*A adapter à sa propre organisation).*

➔ Identifier les principaux acteurs

- **Instances de gouvernance :**
  - Direction générale/ Comité exécutif.
  - Conseil d'administration/ Comité d'audit.
  - Comité éthique et de veille.
  - Comités managériaux.
  - Cellule de crise (Juridique/ Communication/ RH).
  - etc.
- **Moyens de surveillance et de contrôle :**
  - Audit interne.
  - Gestion des risques.
  - Contrôle interne ou contrôle permanent.
  - Ligne managériale (1ère ligne de défense).
  - Services fonctionnels ou support (Communications, Finances, Juridique, Opération, RH, Sécurité, Systèmes d'information).
  - Investigation (Responsable du service, équipe interne, équipe externe).

La valeur ajoutée des fonctions centrales et leurs complémentarités avec les relais locaux est à souligner.

- **Acteurs externes :**
  - Clients/ fournisseurs/ prestataires.
  - Autres acteurs potentiels (Commission Nationale de l'Informatique et des Libertés/ Syndicats/ Police/ Justice/ Autorité des Marchés Financiers, etc.).
  - Audit externe.

➔ Evaluer les procédures et outils

- Charte Ethique / Code de déontologie.
- Charte de la sécurité.
- Politique anti-fraude.
- Mise en place d'un programme pluriannuel de sensibilisation à plusieurs niveaux.
- Procédures d'exception précisant les personnes responsables de l'engagement des actions dérogatoires.
- Procédures disciplinaires.
- Cartographie des risques / *Reporting*.
- Plan de contrôle des composantes du programme et des dispositifs de contrôle anti-fraude.
- Dispositifs de conformité et de contrôle permanent.
- Rapports d'audit interne et externe.
- Base d'incidents / *Reporting*.
- Dispositif d'alerte professionnelle de type « *Whistleblowing* » / *Reporting*[1].
- Protocole de gestion (confidentialité / discrétion).
- Outils de gestion *(Case Management tool) / Reporting.*
- Outils d'analyse / *Reporting*.
- Auto-évaluation du contrôle interne (facilitée ou non par des questionnaires).
- Critères d'excellence opérationnelle.
- Etc.

[1] *Les organisations soumises à la section 301 de la loi américaine Sarbanes-Oxley Act (SOX), juillet 2002.*
En France, les traitements des données concernés par un dispositif d'alerte professionnelle sont légaux s'ils répondent à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne dans les seuls domaines financier, comptable, bancaire et de la lutte contre la corruption. Il s'agit de l'Autorisation unique N°4 (AU-004) de la CNIL du 08/12/2005 http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/declarer-un-fichier/declaration/mon-secteur-dactivite/mon-theme/je-dois-declarer/declaration-selectionnee/dec-mode/DISPLAYSINGLEFICHEDECL/dec-uid/4/

© IFACI

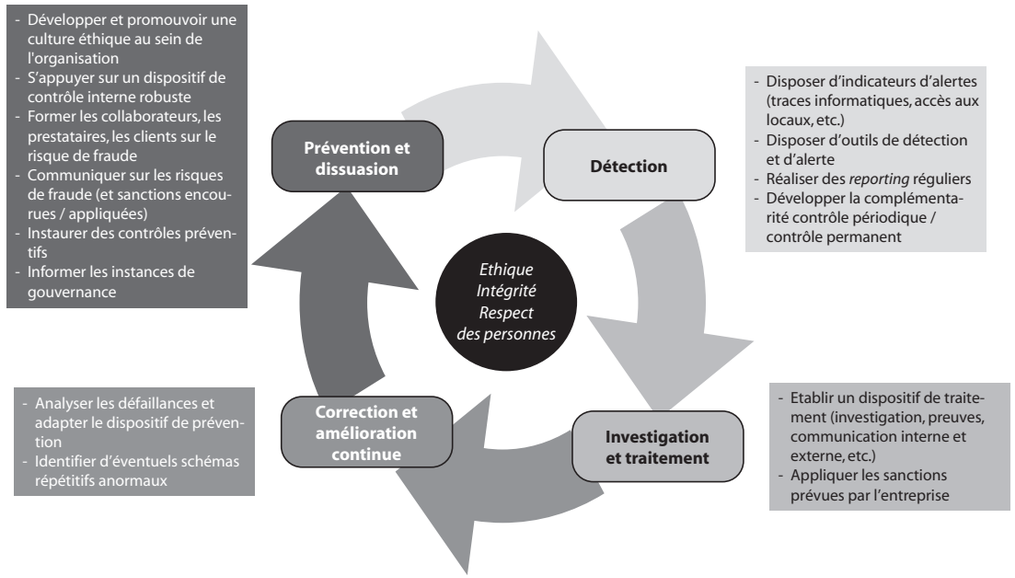
Au-delà de ces outils, le pilotage de la lutte anti-fraude est avant tout une question d'attitude et un état d'esprit et donc repose sur des éléments comportementaux de chacun(e).
Le sens d'observation développé de l'auditeur interne, sa capacité d'écoute, d'analyse et sa connaissance multi-métiers seront primordiaux dans ses recherches. Il ne doit pas soupçonner tout le monde tout le temps, mais être capable d'approfondir l'examen des anomalies sans accepter trop facilement les premières explications. Simultanément il doit être méfiant vis-à-vis des situations et documentations trop idéales qui pourraient cacher une fraude.

3.3- Un pilotage adapté à chaque composante du programme

Un dispositif anti-fraude est généralement structuré autour de quatre composantes, dont l'intitulé varie d'une organisation à une autre :

- la prévention ;
- la détection ;
- l'investigation et le traitement ;
- la correction.

Ces composantes sont schématisées dans la figure ci-dessous :



© IFACI

La **prévention** est le premier maillon du programme de mise en œuvre concrète de la politique diffusée : Comprendre les risques, éviter leur réalisation, expliquer, convaincre.
Le volet prévention est malheureusement insuffisant. Des fraudes sont commises et doivent être détectées au plus vite pour réduire le préjudice subi par l'organisation et les tiers. C'est le volet **détection** du programme anti-fraude.
Sanctionner, voire poursuivre le fraudeur, puis remédier aux dysfonctionnements, tel est l'enchaînement logique de la phase de détection. Cependant, le chemin qui mène de la découverte d'un soupçon de fraude à la fraude avérée ne s'improvise pas. Le **traitement** d'une fraude (de l'investigation aux mesures de sauvegarde) doit être formalisé en tenant compte de la double exigence du cadre légal d'une part et de la confidentialité d'autre part. Cette dernière exigence est en effet nécessaire à la protection des intérêts de l'organisation et de ses représentants.
La communication sur l'ensemble de ce programme et des mesures effectivement mises en œuvre dans l'organisation, concrètement illustrée, tout en se conformant aux règles de confidentialité nécessaires, peut devenir un outil de **dissuasion** puissant.
C'est un **processus évolutif** qui a vocation à s'améliorer de manière permanente au fil de l'expérience acquise.

Compte tenu du caractère global du programme anti-fraude, applicable sur des périmètres très variés d'activité, certaines de ses composantes pourront faire l'objet de la publication de **notes pratiques** ou de **standards** applicables dans toute l'organisation (cf. Partie 3.2, p. 25).

3.3.1. Prévention : des hommes et des risques

Pour mener à bien le volet prévention du dispositif, les objectifs et les modalités d'action suivants sont essentiels :

Objectifs	Modalités d'action
Développer et promouvoir une culture éthique au sein de l'organisation	➔ Diffusion et soutien au plus haut niveau de la démarche éthique de l'organisation. ➔ Diffusion large de la politique anti-fraude.
Définir et diffuser des « standards »	➔ Boîtes à outils pour les animateurs de session de sensibilisation sur la lutte anti-fraude. ➔ Procédures standardisées (méthodologie d'élaboration de la cartographie). ➔ Protocoles de détection ou d'investigation (« qui fait quoi ?» et « comment gérer un soupçon ? »).

© IFACI

Objectifs	Modalités d'action
Sensibiliser les dirigeants, managers, collaborateurs	➔ Les sensibiliser sur : - les risques de fraude et leurs conséquences pour l'organisation et le fraudeur ; - la position à avoir vis-à-vis des différentes parties prenantes (collaborateurs, prestataires, clients) ; - les rôles et responsabilités de chacun. ➔ Prioriser la formation sur les précautions d'usage vers les secteurs sensibles. ➔ Communiquer sur le programme anti-fraude et les conséquences de son application (évolution des risques, effectivité des sanctions, etc.).
Etablir une cartographie des risques de fraude (cf. Partie 5, p. 63)	➔ Assurer une veille sur les risques de fraude. ➔ Identifier les scénarii de fraude pour toute activité/processus de l'organisation. ➔ Evaluer ces scénarii de fraude. ➔ Identifier et évaluer les dispositifs de contrôle en place par scénario. ➔ Evaluer le risque résiduel. ➔ Définir les actions correctives nécessaires. ➔ Assurer un suivi et une revue périodique.
Etablir un *reporting* consolidé des indicateurs de fraude	➔ Constituer une base d'incidents. ➔ Mettre en place un système de *reporting* des cas de fraude. ➔ Consolider les données dans un registre des fraudes avérées. ➔ Analyser et comprendre les scenarii de fraudes avérées. ➔ Construire et suivre les indicateurs de lutte anti-fraude. ➔ Procéder régulièrement à une analyse qualitative et quantitative des éléments de la base d'incidents et du registre des fraudes. ➔ Examiner l'évolution dans le temps des éléments reportés.
Définir la politique d'assurance anti-fraude	➔ Auto-assurance. ➔ Police d'assurance anti-fraude (sectorisée ou globale).
Informer les instances de gouvernance	➔ Rendre compte/reporter les fraudes à la direction générale. ➔ Rédiger un rapport annuel sur le programme anti-fraude. Le présenter au comité d'audit et au conseil d'administration. ➔ Mettre en place des procédures spécifiques d'escalade pour certaines typologies de fraude.

© IFACI

Objectifs	Modalités d'action
S'assurer de la bonne mise en œuvre des dispositifs de contrôles préventifs prioritaires	➔ Au niveau des ressources humaines : - vérification des antécédents et des références lors des recrutements, - gestion des mobilités. ➔ Dans le cadre des règles de sécurité : - règles de délégation, - séparation des pouvoirs, - procédures de traçabilité et d'autorisation : double validation, contrôle physique et logique des accès (enregistrement des transactions, confirmations, limites, contrôle a priori préventif, contrôle a posteriori). ➔ Avec la sécurisation des SI (gestion des habilitations, accès, droits, profils)[1]. ➔ Dans le cadre d'une politique de conformité (ex : conformité aux exigences de la CNIL) et de confidentialité pour les dispositifs anti-fraude sensibles (inspections, investigation, surveillance, détection proactive, reportings, *whistleblowing*, etc.). ➔ etc.

3.3.2. Détection : contrôler pour stopper ou découvrir vite

En dépit de la qualité des systèmes de prévention mis en place, tous les cas de fraude ne peuvent pas être évités et leur détection reste très difficile. L'optimisation de cette étape vise à raccourcir le temps nécessaire pour l'identification de la fraude. A cet effet, il convient d'accroître la complémentarité contrôle périodique/ contrôle permanent. Rappelons que le contrôle permanent s'appuie à la fois sur les compétences métiers des opérationnels et sur le contrôle de second niveau assuré par une équipe dédiée (conformité, contrôle interne, etc.).

La détection est une résultante de la prévention qui :

- augmente le niveau de vigilance vis-à-vis de la fraude (un opérationnel sensibilisé sur le risque de fraude détectera des incohérences par rapport au cours normal des activités, or ces écarts peuvent être des indices de fraude, etc.) ;
- développe l'esprit critique en évitant de se contenter des explications superficielles données pour justifier certains écarts ou certaines attitudes ;
- incite à documenter l'explication des écarts et à ne pas transformer toute anomalie en soupçon de fraude, voire en fraude avérée ;
- facilite la remontée des soupçons vers les services qui doivent les traiter (cf. Partie 4.4, p. 47).

Lorsque le nombre de transactions le justifie, des outils informatiques peuvent être utilisés pour détecter des anomalies à analyser :

➔ dispositifs de contrôles détectifs (blocage, listes d'anomalies, vérification du respect de toutes les validations et de leur seuil de déclenchement, etc.) ;

[1] *Global Technologie Audit Guide (GTAG) 9 : Gestion des identités et des accès, IIA/IFACI*

© IFACI

➔ programme de recherche de données ou de transactions anormales a posteriori (outils d'audit en continu).

Les acteurs de la détection doivent savoir être attentifs aux signaux faibles et à certains comportements inhabituels. Ce sont cette vigilance et cette ouverture d'esprit qui leur permettront de réagir rapidement.

Facteurs d'un environnement organisationnel augmentant les risques de fraude (cf. Partie 1.3, p. 17) :

- Trop de latitude donnée à des fonctions clés.
- Absence de procédures pour les autorisations de transactions.
- Manque de séparations des tâches sur les fonctions clés.
- Absence de contrôle indépendant des performances.
- Pas de contrôle des détails.
- Absence d'organisation claire de l'autorité et des responsabilités.
- Absence de mission de l'audit sur les départements.
- Rotation insuffisante du personnel à certains postes clés.

Facteurs relatifs aux caractéristiques personnels d'un individu augmentant le risque de fraude :

- Un train de vie supérieur aux ressources de l'individu.
- Un attrait pour l'argent.
- Le surendettement.
- De trop bonnes relations avec les tiers (clients, fournisseurs).
- Une mauvaise opinion sur son salaire.
- Une envie de défier le système.
- Une réputation de joueur.
- Des problèmes familiaux.
- Absence de reconnaissance des efforts fournis.

Source : Deterring Fraud : The internal auditor's perspective, Steve Albrecht

La documentation des procédures de détection est un excellent moyen de capitaliser l'expérience pour des analyses sur des cas similaires et la réplication à l'échelle d'un groupe.

Ces indicateurs devront être utilisés avec une très grande prudence et corroborés par des faits avérés pour ne pas être entraîné dans une sorte de paranoïa ou se laisser emporter par des préjugés, voire des procédés illégaux prohibés notamment en matière de protection des données personnelles.

© IFACI

Point de vigilance juridique : Données personnelles

L'atteinte aux données à caractère personnel est sanctionnée principalement par les articles 226-16[1] et suivants du Code pénal. Pour les données personnelles intégrées à un système informatique, il convient également de se conformer à des dispositions légales spécifiques, introduites dans le Code pénal (articles 323-1[2] à 323-7) par la loi dite « Godfrain » ainsi que par la loi du 5 janvier 1988 relative à la fraude informatique.
Mais les règles du droit pénal ne sont pas le seul dispositif applicable. Les entreprises doivent également prévoir et faire appliquer des chartes d'utilisation des moyens informatiques (ordinateurs, périphériques amovibles, logiciels, Internet, etc.) et des politiques de sécurité pour la protection des données à caractère personnel (salariés, prospects, clients, fournisseurs, etc.).

Pour la mise en place de ces mesures de sécurité, les entreprises doivent dresser un inventaire formel de toutes les législations et réglementations qu'elles sont tenues de respecter dans leurs différents lieux d'implantation. Par exemple, les systèmes d'alerte professionnelle anti-fraude (*whistleblowing system*), requis par la loi américaine Sarbanes Oxley, sont strictement encadrés en France. Selon l'objet et la finalité du dispositif, l'entreprise devra engager auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) :

- une procédure administrative préalable de déclaration[3] ou,
- une procédure administrative préalable d'autorisation[4].

Le récépissé de déclaration ou d'autorisation de la CNIL doit avoir été obtenu par le déclarant avant la mise en œuvre du système d'alerte.

Il convient également de recenser et de prendre en considération les besoins de sécurité anti-fraude liés aux différentes activités et métiers de l'entreprise.
A cet effet, il est recommandé la désignation de spécialistes, référents[5] internes ou externes avec lesquels l'entreprise pourra travailler et s'assurer à tout instant du respect des règles du droit informatique et de la protection des données à caractère personnel.

---

[1] *Article 226-16 du Code Pénal Modifié par la Loi n°2004-801 du 6 août 2004 - art. 14 JORF 7 août 2004*
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »
« Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »
Cité par la Loi n°78-17 du 6 janvier 1978 - art. 45 (M) et la Loi n°78-17 du 6 janvier 1978 - art. 50 (V)

[2] *Article 323-1 du Codé Pénal Modifié par la Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004*
« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. » « Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. »

[3] *Conformément à l'adoption de la décision d'autorisation unique édictée par la CNIL le 8 décembre 2005, également couramment dénommée « autorisation unique n°4 ».*

[4] *Dans un arrêt du 8 décembre 2009, la chambre sociale de la Cour de cassation a rappelé que les systèmes d'alertes professionnelles autorisées par la CNIL dans le cadre de « l'autorisation unique n° 4 » doivent avoir un champ d'application strictement limité.*

Toutefois, cette décision ne remet pas en cause le principe même des dispositifs d'alertes professionnelles qui continuent à pouvoir être mise en place par les entreprises, sous réserve du respect des limites indiquées par la CNIL sous le contrôle des juridictions compétentes.

[5] *Il a été ainsi confirmé par la CNIL et approuvé par le Conseil National des Barreaux (Rapport présenté par Me Guillaume Le Foyer de Costil à l'Assemblée générale du CNB du 14 mars 2009), que l'avocat peut être désigné en qualité de Correspondant Informatique et Libertés (CIL) dans une entreprise. L'avocat qui agit en qualité de CIL, n'a aucune obligation de dénonciation directe des insuffisances de l'entreprise ou du responsable des traitements. L'avocat est plus dans la position d'un expert qui rend compte de sa mission à son client.*

© IFACI

3.3.3. Investigation et traitement : établir les éléments factuels et sanctionner les auteurs

Traiter efficacement un cas de fraude supposée commence par la maîtrise du circuit d'information en amont. La source d'information initiale peut être interne à l'organisation (contrôle managérial, mission d'audit, alerte d'un salarié, etc.) ou externe (réclamation client ou fournisseur, police, justice, médias, etc.). La règle de prudence veut que la personne qui va prendre connaissance ou détecter des faits susceptibles de recouvrir une fraude au sein de l'organisation, les fasse parvenir à l'instance de l'organisation, dotée des pouvoirs pour procéder au traitement, avec le degré de confidentialité et l'encadrement juridique nécessaire. Par principe, aucun employé ne doit procéder à une enquête de sa propre initiative.
L'expérience enseigne que chaque cas de fraude est spécifique. Cependant, la démarche générale de traitement d'un cas, qui ne se limite pas seulement à l'investigation, peut être assimilée à la gestion d'un projet, dont l'objectif est d'évaluer des risques, de confirmer ou infirmer des faits par la recherche de preuves, d'établir des responsabilités, de prendre des actions de sauvegarde des intérêts de l'organisation, de décider en cas de fraude avérée des sanctions disciplinaires et poursuites judicaires ad hoc, d'assurer la bonne comptabilisation et le bon suivi du cas jusqu'à décision de clôture, d'effectuer le *reporting* nécessaire et, le cas échéant, d'activer les procédures d'escalade. Cette démarche nécessite des acteurs compétents, indépendants, aux pouvoirs clairement établis. Confidentialité et respect de la législation (droit social, Informatique et Libertés) sont également deux principes incontournables.
Plusieurs possibilités s'offrent à l'organisation mais en général, la responsabilité du traitement des cas est confiée soit à un responsable opérationnel, à l'audit, à la direction juridique ou à une direction de la sûreté qui peut disposer des moyens nécessaires. Nous nous référerons au **Responsable du traitement**. Pour certains cas, il peut être admis par l'organisation que le management et la DRH procèdent au traitement. Le responsable du traitement définit le circuit de *reporting* de suivi de l'avancement du cas, en veillant à préserver l'anonymat et la confidentialité des informations diffusées.
Il est conseillé à l'organisation de rédiger le cadre de la démarche du traitement d'un cas supposé dans un « guide de traitement », validé par la direction de l'organisation. Ce cadre a pour but de définir les rôles et responsabilités, puis d'en détailler les étapes, faisant également office de *check-list*. On peut distinguer 5 grandes étapes du traitement d'un cas de fraude supposée :

1. **Evaluation du risque**
2. **Organisation du traitement et prise de mesures d'urgence**
3. **Investigation**
4. **Décisions de l'organisation**
5. **Suivi du cas / Clôture**

Le lecteur trouvera dans la partie 4 (p. 35) une démarche pour réagir à un soupçon de fraude et le traiter.

© IFACI

3.3.4. Correction : éviter la répétition

Chaque cas de fraude doit faire l'objet d'une analyse a posteriori afin d'en tirer des enseignements et ainsi éviter la répétition de procédés similaires au même endroit ou dans des entités similaires (filiales / succursales par exemple), par la mise en place d'actions correctives. Pour chaque cas, les questions suivantes peuvent se poser :

- Peut-on éviter la répétition du cas par des mesures de prévention ?
  - Exemple : formation des managers, mise en place d'états d'exception, de contrôles bloquants, etc.
- Peut-on le détecter plus vite ?
  - Exemple : programme d'analyse de données.
- La faille découverte aurait-elle pu être plus grave ?
  - Exemple : Un cas de fraude de faible coût stoppé par hasard ou par la maladresse du fraudeur peut révéler des déficiences de contrôle très significatives.

Il sera difficile de trouver les réponses à ces questions sans une explication claire du déroulement de la fraude et des faiblesses ayant permis sa survenance (cf. Partie 6, p. 77). La mise en place des actions correctives fera l'objet d'un suivi rigoureux.
Les options prises et les mots choisis participeront à la compréhension de la politique éthique de l'organisation. Le dosage dans le positionnement : prévention, dissuasion voire répression, appartient à chaque organisation et conditionnera le programme anti-fraude. Quelles que soient les étapes privilégiées, il convient de passer d'un mode réactif à mode proactif.

Base des incidents :
Il est utile de constituer une base des incidents recensant les cas traités : les données chiffrées, les descriptifs des procédés frauduleux, les déficiences éventuelles enregistrées, les actions correctives, les sanctions et jugements. Cette base de données peut servir à :

- identifier d'éventuels schémas répétitifs anormaux ;
- enrichir la qualité de la revue d'évaluation annuelle des risques de fraude (cartographie) grâce à la meilleure connaissance des causes et conséquences des cas ;
- évaluer dans le temps l'évolution de l'efficacité du dispositif anti-fraude :
  - analyse glissante d'indicateurs (modes de détection, délais de détection, etc.),
  - analyse d'efficacité du traitement (application des sanctions, etc.),
  - etc.
- fournir des éléments pour améliorer la communication interne ou les études de cas avec les opérationnels.

La pertinence et la fiabilité des informations contenues dans cette base devront être évaluées.

© IFACI

Partie 4

Réagir face à un soupçon de fraude ou traiter un cas avéré

La mise en place proactive des étapes du dispositif de lutte anti-fraude présentées dans la partie précédente permet d'agir efficacement et rapidement. Ce dispositif global peut ainsi être appliqué et adapté lorsqu'un cas particulier de fraude est soupçonné ou avéré.

© IFACI

© IFACI

4.1- Pré-requis pour mener une investigation

Pour bien réagir à la remontée d'un soupçon de fraude, il y a un certain nombre d'éléments qui, idéalement, devraient être en place. Bien entendu, il faudra considérer la taille de l'organisation, l'environnement dans lequel cette dernière évolue ainsi que sa culture interne et donc adapter les recommandations aux spécificités de chaque organisation. Nous décrivons ci-dessous ces pré-requis.

4.1.1. Disposer de modalités de remontée des soupçons claires et connues.

De façon générale, la gestion des soupçons devrait être gérée comme une situation de crise. Il s'agit donc d'anticiper cette situation de crise en mettant en place des modalités de remontée claires et connues, et disposer d'une organisation définie de gestion de crise.

4.1.1.1. Anticipation – un management alerté et conscient du risque de fraude

Dans le domaine de la gestion de la fraude, il est important de ne pas être naïf et donc d'anticiper cet événement, sachant qu'éventuellement l'organisation en sera victime. Il s'agit donc de préparer les managers à cette situation et de leur faire prendre conscience des risques.
Il faut aussi savoir que les premiers touchés sont souvent les opérationnels et ceux-ci doivent se préparer à la potentialité d'événements, telles la rumeur de fraude, la divulgation de fraude, bref la capacité à comprendre la gravité des faits et comment y réagir.
Cette prise de conscience doit aussi être adaptée au contexte local des managers, car le risque de fraude peut être différent selon les environnements.

4.1.1.2. Canaux de remontées des informations

Il est important d'avoir des canaux de remontée d'informations claires pour pouvoir ensuite gérer efficacement les informations concernant des soupçons de fraude. Il existe plusieurs canaux de remontée des soupçons de fraudes tels que les opérationnels, le management, l'audit interne, l'audit externe, la surveillance et la dénonciation.
Il est, bien entendu, important de promouvoir un climat de travail où les employés vont se sentir à l'aise pour remonter un soupçon à leur supérieur hiérarchique. Cependant, dans certains cas, l'employé préfère le faire en dehors de la voie hiérarchique. Ainsi, la mise en place de dispositif d'alerte professionnel bien maîtrisé peut permettre une remontée rapide et confidentielle de l'information. Elle permet non seulement aux employés, mais aussi aux fournisseurs, clients, compétiteurs et autres tiers, de remonter les soupçons à l'organisation. De plus, des « lignes éthiques »[1] peuvent être mises en place pour permettre une remontée via téléphone, e-mail ou encore au

[1] *La section française de Transparency International a recensé tous les textes législatifs sur le dispositif d'alerte éthique ou whistleblowing en France. www.transparency-france.org. De plus, la résolution 1729 et la recommandation 1916 du 29 avril 2010, encouragent les Etats à légiférer sur la protection des whistleblowers.*

© IFACI

travers d'Internet. Attention, ces canaux de remontées d'information ne sont pas acceptés dans tous les pays (contraintes juridiques ou culturelles), il faut se renseigner sur les possibilités auprès de la direction juridique et des ressources humaines.

Enfin, pour assurer l'efficacité du processus, il faut organiser des campagnes de sensibilisation et communiquer régulièrement sur l'existence de la ligne éthique.

4.1.1.3. Disposer d'un document de référence avec des procédures écrites

La démarche proposée est similaire à celle qui est mise en œuvre dans le cas d'un plan de continuité d'activité (PCA). Elle a pour but de définir les rôles et responsabilités, de détailler les étapes clés et leurs modalités de contrôle.

Une procédure écrite incluse dans ce document permet non seulement de formaliser mais aussi de diffuser l'information, qui pourra ainsi être traitée plus efficacement.
Cette procédure devrait être en relation avec le code de conduite de l'organisation :

- clarifier les règles pour la remontée des informations selon les sources (établir un document type) ;
- définir à qui l'information devrait être remontée (management, audit, juridique, etc.) ;
- prévoir les délais de remontée après la découverte (le cas échéant, les délais devraient prendre en compte les modalités du contrat d'assurance contre la fraude) ;
- prévoir des seuils de matérialité ou encore demander la remontée systématique de tout soupçon sans égard à la matérialité ;
- prendre en compte les dispositions et obligations légales et statutaires telles que la confidentialité de l'information, la protection des individus et de leur réputation, la remontée de l'information au comité d'audit, etc.

4.1.1.4. Gérer le canal assurance

Il existe divers contrats d'assurance, dont ceux qui visent à traiter les risques de fraude. Ils font souvent partie des pré-requis souhaitables, mais il appartient à l'organisation d'envisager d'en prendre une en fonction de la cartographie des risques.

Si une assurance fraude est retenue, ses modalités devraient être prises en compte dans la procédure interne de gestion de fraudes pour s'assurer qu'une éventuelle réclamation sera bien recevable par l'assureur.

4.1.1.5. Mettre en place un registre des fraudes

La mise en place d'un registre des fraudes est un outil indispensable qui permet un suivi adéquat de l'évolution des fraudes au sein de l'organisation en permettant de répertorier et de suivre les situations récurrentes. Il permet également de faire du *benchmark* entre les différents cas (cf. Bonnes pratiques sur la base des incidents, p. 34).

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

La gestion par des moyens simples (feuille de calcul) est possible, mais en fonction des besoins, il faudra étudier l'utilisation de logiciels plus élaborés de gestion des cas qui se développent actuellement sur le marché.

4.1.2- Disposer d'une organisation de gestion de crise connue et mobilisable dans les délais requis pour traiter les incidents

Des structures de gestion permanente des risques de fraude doivent être envisagées pour les anticiper et s'en prémunir efficacement. Elles permettront également de gérer les incidents qui n'ont pas pu être évités et de capitaliser les retours d'expérience. Cette structure sera adaptée à l'organisation et aux circonstances (taille, métiers, perception du risque, etc.).

4.1.2.1. Anticipation

Nous avons déjà mentionné l'importance de l'anticipation dans la gestion de la fraude. En effet, lorsqu'un soupçon de fraude remonte, il s'agit d'un évènement perturbant dans la conduite des affaires quotidiennes. Ce dernier ne peut être ignoré et doit être traité dans un délai approprié, d'où l'importance de préparer la gestion de crise avec une organisation bien définie. La mise en place d'une gestion de crise liée à une fraude est assimilable à une gestion de crise de type sinistre (plan de continuité d'activité).

4.1.2.2. Organisation de gestion de crise

Il s'agit de mettre en place un comité en charge de traiter les soupçons. A minima, il devra inclure un membre du département Juridique et de l'Audit interne. Ensuite, selon l'organisation, on pourra identifier des intervenants internes (Ressources Humaines, Sécurité, Communication, etc.) et externes qui seront sollicités, selon le cas et les besoins.
Il faut prévoir un dispositif de communication de crise permettant de contrôler les informations qui parviennent aux médias et entraîner les personnes amenées à communiquer à le faire efficacement.

4.1.2.3. Responsabilités définies

Définir le « qui fait quoi » par anticipation, plutôt que d'improviser dans des moments critiques. Idéalement, il est préférable d'avoir aussi sélectionné ou du moins identifié les acteurs externes potentiels. En effet, il peut arriver que l'expertise ne soit pas disponible en interne nécessitant alors l'emploi d'experts du type détective privé, experts en investigation de fraude (cabinet Forensic ou pour les sociétés d'assurance, le recours à l'ALFA - Agence pour la Lutte contre la Fraude à l'Assurance), etc. Dans ce cas, il est important d'avoir identifié un collaborateur pour piloter le mandat et assurer le suivi des étapes.
Enfin, dans certains cas, il se peut qu'il faille aussi contacter les autorités administratives et/ou judiciaires.

© IFACI

L'identification préalable des intervenants et la sélection des fournisseurs assureront une réponse rapide le moment venu.

4.1.2.4. Les bons réflexes

L'objectif de la mise en place d'une organisation ou d'un comité de gestion de la crise est d'assurer les bons réflexes et entre autres :

- la gestion de la confidentialité des informations (Protection de la vie privée, CNIL, etc.) ;
- la cascade de l'information après avoir défini qui peut ou doit être mis au courant des soupçons ;
- la compréhension de l'environnement légal local, des sanctions et mesures disciplinaires qui peuvent être prises ;
- l'analyse « stratégique » du soupçon (enjeu de la fraude possible pour le Groupe, les implications possibles, etc.) ;
- la communication de crise interne et, si nécessaire, une communication externe approprié.

4.1.2.5. Les enjeux administratifs

Il y a bien sûr certains enjeux administratifs à considérer :

- inclure des tiers tel l'assurance et gérer en fonction des obligations contractuelles (Ex : contrat d'assurance fraude ou vol, délais pour informer de l'incident, franchise, etc.) ;
- établir le budget potentiel (si recours à des personnels extérieurs ou si mobilisation de personnel) et dans quel cas il y aurait recours à ce genre de ressources (ex : type de fraude, enjeux de la fraude, etc.) ;
- maîtriser les processus de demandes d'informations comptables (demandes d'achats, facturation) pour garantir la confidentialité. Il faut en effet payer les fournisseurs qui participeraient à l'enquête.

En conclusion, la mise en place de ces éléments conjointement avec une anticipation adéquate constitue les pré-requis importants pour bien réagir à un soupçon de fraude. Il est aussi important de bien former les managers sur la thématique fraude et surtout, étant donné les enjeux, d'éviter qu'ils agissent seuls.

© IFACI

4.2- Phase de découverte d'une anomalie

De par sa fonction et sa connaissance de l'organisation, l'audit interne est régulièrement informé des faits et actes anormaux significatifs présents au sein de son organisation.

Dans le cadre de cette veille permanente, il peut être confronté à la découverte d'un soupçon de fraude ou d'une fraude avérée.

Au-delà du premier effet de surprise, l'audit interne devra faire preuve de réactivité en mettant en place un certain nombre d'actions « réflexes », qui lui permettront d'organiser et de gérer la situation.
Il devra, dès le début des premières investigations, porter une attention particulière à la fiabilité des informations recueillies et s'assurer également de leur pertinence.

Ces principales actions « réflexes » à mettre en œuvre consisteront à :

- collecter toutes les informations disponibles au sein de l'organisation pour pouvoir faire une pré-analyse des faits ;
- faire une première évaluation des risques ;
- informer la hiérarchie sur la découverte d'un risque majeur potentiel ou réel.

4.2.1. Principales sources d'information

Les informations relatives au soupçon de fraude ou fraude avérée peuvent provenir de plusieurs sources, dont aucune n'est à écarter :

- management ;
- opérationnels ;
- tiers externe ;
- contrôle permanent ;
- réclamations clients/ fournisseurs/ partenaires ;
- dispositif d'alerte professionnelle ;
- contrôles automatisés (gestion des profils, analyse de données, blocages, etc.) ;
- voix non officielles (rumeurs, etc.).

En pratique, les premières informations disponibles sont souvent complétées et recoupées avec d'autres, car le but recherché est d'identifier et de retenir uniquement les faits (cf. Point de vigilance juridique : Données personnelles, p. 32).

© IFACI

Le soupçon de fraude peut résulter d'un signalement par un interlocuteur identifié qui déclare des actes et des données qu'il juge anormaux. Les managers et les autres destinataires de ces informations doivent être attentifs et encourager la transparence.

Certaines informations pourront quelquefois être difficiles à collecter, en fonction des organisations et des dispositifs délégataires (délégations de pouvoir) associés en place (métiers, géographie, nombre de niveaux de management/ délégation pour agir, etc.). Il appartiendra alors à l'auditeur interne de veiller à lever ces premiers « barrages » sans délai afin d'obtenir, dès le début de ses investigations, des informations factuelles, exploitables et fiables.

4.2.2. Première évaluation des risques

Les informations factuelles retenues doivent permettre de donner des indications précises sur la nature (faits caractérisés, personnes identifiées, etc.) et la provenance du soupçon. A ce stade, toutes les informations doivent être prises en considération, quel que soit leur niveau de détail, afin d'évaluer le mieux possible la consistance et le niveau de risque réel ou potentiel associé au soupçon de fraude.
Cette étape est essentielle, car elle permet de mieux définir un cadre de traitement (gestion opérationnelle, communication interne, relation médias et autorités, procédures disciplinaires et judiciaires, etc.), de mobiliser ou d'informer sans délai les bons interlocuteurs et de prendre les mesures d'urgence nécessaires. L'appréciation du risque doit comporter des données chiffrées, mais aussi tenter d'évaluer, par exemple, un risque de réputation, de collusion interne ou externe, etc.
Cette première évaluation des risques n'est pas destinée à être figée et devra naturellement évoluer en fonction des informations complémentaires qui viendront alimenter le soupçon de fraude tout au long des investigations.

Il est indispensable de mettre en place un système proactif d'analyse des données recueillies.

4.2.3. Quelques autres précautions à prendre

Il sera utile d'identifier et de neutraliser rapidement les éventuels conflits d'intérêts entre collaborateurs afin de préserver l'objectivité des constats de l'audit interne et d'éviter tout risque d'erreur. Il faut également prendre en compte la possibilité que le fraudeur ne soit pas seul à agir et qu'il existe une collusion interne ou externe. La stratégie doit être adaptée et la confidentialité renforcée.

© IFACI

La confidentialité sera une préoccupation permanente pour ne pas éveiller les éventuels soupçons du fraudeur qui pourrait effacer certaines preuves ou pour protéger la personne soupçonnée sans fondements (cf. Partie 4.2.1, p. 41).

4.2.4. Premiers échanges avec la direction générale

Cette première étape « Phase de découverte » peut se conclure par l'identification d'un ou plusieurs risques majeurs réels ou potentiels tels que, par exemple :

- des pertes financières significatives ;
- une atteinte à la notoriété.

Selon les modalités définies dans les pré-requis sur les modalités de remontée des informations, le responsable du traitement prendra contact avec la direction générale, avant la phase de pré-investigation, pour un échange formel. Il présentera les premiers éléments factuels recueillis ainsi que les risques majeurs identifiés.
Cette démarche permettra d'être soutenue dans la suite des investigations à mener.

© IFACI

4.3- Phase de pré-investigation

La phase de pré-investigation consiste pour l'auditeur à rassembler les premiers éléments de soupçon de fraude recueillis au cours de la phase de découverte et à procéder à une phase d'analyse des données.
Cet exercice doit déboucher sur une évaluation de la consistance du soupçon.
Il s'agira, entre autre :

- d'organiser les informations collectées par typologie ;
- de documenter les faits retenus ;
- de préciser les risques ;
- de comprendre les mécanismes utilisés ;
- d'identifier les personnes concernées ;
- d'identifier les « zones d'ombre » non expliquées.

Il n'existe pas de plan de travail type qui puisse garantir la qualité des travaux à mener dans le cadre de la phase de pré-investigation.
En pratique, l'idéal serait de mettre en place des outils du type tableaux synoptiques, fiches de synthèse, schémas à remplir, afin de mieux cerner le soupçon de fraude.

Ces supports de travail pourront être utilisés tout au long du processus du traitement de la fraude et devront être régulièrement mis à jour. Il est important de conserver l'historique des points de passage réalisés car ces derniers pourront être réutilisés à tout moment.

4.3.1. Exemple de feuille d'analyse du soupçon de fraude en phase de pré-investigation

Feuille d'analyse du soupçon de fraude en phase de pré-investigation :

Principaux constats et analyse concernant le soupçon de fraude	• Commentaires détaillés sur la nature de la découverte. • Analyse du soupçon de fraude. • Analyse du processus. • Date, historique, évaluation de la matérialité, analyse de la cohérence des faits, etc. • Identifier les parties prenantes (initialiser un logigramme).
Identification des points non éclaircis	• Identification des « zones d'ombres ». • Incompréhension de certains faits et motifs.
Mesure des risques, des enjeux et des conséquences	• Identifications des risques majeurs. • Identification des risques mineurs (ils peuvent révéler des failles à maîtriser ; la répétition de l'incident peut en faire des risques majeurs). • Premières évaluations du ou des préjudices.
Identification des motivations des éventuels fraudeurs	• Identifier les liens entre les personnes. • Comprendre le rôle de chacun.
Principales actions proposées ou déjà mises en œuvre par rapport à ce soupçon de fraude	• Actions mises en œuvre en urgence pour neutraliser les risques perçus. • Actions proposées pour mise en œuvre ultérieure.
Evaluation de la consistance d'un soupçon de fraude	• Résultat de la simulation du soupçon de fraude. • Premières conclusions. • Premiers axes de recherche à mettre en place pour compléter les informations sur le soupçon de fraude. • Identification des besoins.

4.3.2. Représentation conceptuelle du schéma de fraude : le logigramme

L'objectif de ce support est de permettre à son lecteur de comprendre très vite, avec une vue d'ensemble, les principaux éléments du processus mis en place par les éventuels fraudeurs.

Ce schéma doit répondre de façon visuelle notamment aux questions suivantes :

- Quelles sont les principales étapes du processus fraude détecté ?
- Quelles sont les personnes (interne / externe) concernées ?
- Les délais entre les actions menées par le ou les fraudeurs.
- Les zones de risques (failles : mineures, majeures, etc.).

Il est important de mettre à jour régulièrement le logigramme en indiquant les avancées et en historisant les différentes versions. Ce logigramme sert alors de tableaux de bord.

4.3.3. Approche intuitive

Le sujet de la fraude est sensible, mais également complexe. Les fraudeurs ont beaucoup d'imagination, c'est pourquoi il ne faut pas rejeter l'approche intuitive.
En se mettant à la place du fraudeur, l'auditeur devra dérouler le processus identifié pour s'assurer de sa cohérence. Cette démarche doit impérativement être complétée par le recueil des faits.

© IFACI
© IFACI

4.3.4. La phase de remontée de l'information

A l'issue de la phase de pré-investigation, le responsable de l'investigation doit informer sa hiérarchie directe et la direction générale sur ses conclusions et ses propositions.

Il est indispensable de formaliser la démarche par un document qui reprendra les principales étapes qui ont conduit aux conclusions.
Les éléments doivent être factuels et documentés pour la bonne compréhension du décideur.
Il peut s'agir de :

- la feuille d'analyse du soupçon de fraude en phase de pré-investigation ;
- le résumé des faits ;
- le détail des montants concernés ;
- la liste des actions déjà mises en œuvre ;
- la liste des actions à mettre en œuvre pour éviter une récidive.

© IFACI

4.4- Evaluation des enjeux et calibrage des moyens

Selon les modalités de gestion de la crise, le comité décisionnaire évalue, à partir de la pré-investigation, les dispositions à mettre en œuvre pour conduire les investigations et prendre les mesures conservatoires adaptées.

L'analyse initiale doit permettre de définir a minima :

- les précautions à prendre en termes de confidentialité ;
- les ressources nécessaires pour conduire les investigations ;
- l'organisation des travaux et les responsabilités ;
- la nature et le niveau de *reporting* qui devront accompagner l'avancement de l'enquête.

Cette analyse prendra notamment en compte :

- les principes retenus par l'organisation en matière de lutte contre la fraude (ex : tolérance zéro, seuils de matérialité ou existence de seuils de gravité, de rapport bénéfice/coûts, etc.) ;
- la nature des parties prenantes soupçonnées (individu, crime organisé, etc.) ;
- les conséquences possibles de la fraude concernée si elle était avérée (conséquence financière, image, exemplarité, etc.) ;
- le risque de disparition de preuves ;
- la violation de la loi ou des règles de l'organisation.

4.4.1. Précautions en termes de confidentialité

Celles-ci doivent être appréciées au regard de l'impact potentiel de la fraude soupçonnée sur l'organisation. Plus l'impact potentiel sur l'organisation sera important, plus il sera essentiel de préserver la confidentialité tout au long des investigations afin, en particulier, de permettre à l'organisation de garder la maîtrise de la communication.
La confidentialité est également indispensable pour réduire le risque d'alerte des éventuels fraudeurs et les destructions de preuve associées.
Par ailleurs, la confidentialité est indispensable pour protéger d'éventuels témoins des pressions possibles, soit pendant la période d'investigation soit ultérieurement, en particulier en cas de fraudes graves ou organisées.
Enfin, la confidentialité est importante, dans l'hypothèse où le soupçon ne serait pas avéré, pour protéger les personnes indûment soupçonnées, en particulier pour préserver leur réputation.
Au titre de ces précautions, le responsable désigné veillera à limiter au strict nécessaire le nombre de personnes sollicitées dans le cadre de l'investigation et/ou destinataires du *reporting*. En outre, il pourra utilement :

- établir la liste exhaustive des personnes informées ;

© IFACI

- obtenir, de tous ceux qui ne sont pas explicitement engagés de par leur responsabilité dans l'organisation, un engagement de confidentialité ad hoc ;
- définir les conditions de mise à disposition des documents utiles (espace sécurisé, encodage d'envois dématérialisés, protection des documents papiers, etc.).

4.4.2. Les ressources nécessaires pour conduire les investigations

Les ressources à mobiliser doivent tenir compte d'une part des besoins d'investigation et d'autres part des besoins de traitement de la fraude et de ses conséquences, dans l'hypothèse où elle serait avérée.
Pour l'investigation, les ressources utiles peuvent être soit sollicitées au sein de l'organisation soit être mandatées en externe. Elles concernent principalement :

- les compétences techniques permettant d'investiguer les processus concernés :
  - spécialiste du métier concerné (gestion de stocks, *trading*, processus client, etc.) ;
  - expert informatique pour extraire des données ;
  - expert télécom.
- les compétences juridiques ou administratives permettant de garantir la robustesse du dossier constitué sous tous ses aspects (délais, conformité, respect des conventions collectives, respect des lois relatives aux données et à l'informatique, etc.) :
  - juriste d'organisation ;
  - avocats ;
  - huissier de justice ;
  - autorités juridiques, administratives ou de police ;
  - régulateurs ou autorités des marchés sectoriels concernés (financier, télécom, concurrence, immobilier, énergie, etc.).
- les spécialistes de l'investigation :
  - détective ;
  - auditeurs internes ;
  - éventuelle(s) fonction(s) dédiée(s) à la fraude.
- des parties prenantes de la fraude soupçonnée, tant en interne qu'en externe, en particulier lorsque le soupçon concerne la corruption ou le crime organisé (autres victimes de la fraudes, témoins possibles, etc.).

Pour le traitement des conséquences de fraude, les principales ressources qu'il convient d'envisager, en complément des ressources déjà mobilisées dans le cadre de l'investigation elle-même, sont :

- dans le cas d'une fraude interne, l'interlocuteur RH (gestionnaire des cadres dirigeants, DRH, manager concerné, etc.) qui aura à instruire d'éventuelles suites relatives au contrat de travail (mesure disciplinaire, licenciement, etc.) ;
- l'interlocuteur de l'assurance de l'organisation et, le cas échéant, l'assureur lui-même ;

© IFACI

- l'interlocuteur en charge de la communication externe ;
- le cas échéant, s'il est différent des personnes déjà mobilisées, l'interlocuteur qui sera en charge de la communication interne ;
- les interlocuteurs qui seront chargés de mettre en œuvre les éventuelles mesures conservatoires (cf. Partie 4.5, p. 50).

Outre ces ressources spécialisées, il convient, comme pour un projet, d'identifier les ressources logistiques, éventuellement nécessaires, pour l'ordonnancement d'ensemble (gestion des contrats externes, gestion des ressources financières, archivage et protection des documents, des enregistrements et des éléments matériels, interfaces entre les interlocuteurs « qui ne devraient pas se croiser », demandes d'accès -codes, documents classifiés, etc.).

Dans tous les cas, le risque de conflit d'intérêt sera analysé avant la sollicitation effective d'une ressource pressentie, en particulier en cas de soupçon concernant des dirigeants.

4.4.3. La nature et le niveau de reporting qui devront accompagner l'avancement de l'enquête

Malgré la nécessaire confidentialité qui doit accompagner l'ensemble des investigations (cf. Partie 4.1, p. 31), les conséquences potentielles d'une fraude en termes d'image – tant externe qu'interne- mais également en termes financier justifient que la direction générale et les acteurs de la gouvernance (comité d'audit, etc.) concernés soient informés de façon régulière et adaptée.
Dans l'hypothèse où les pré-requis le prévoient (cf. Partie 4.1.2, p. 39), les interlocuteurs concernés et la forme du *reporting* sont prévus au préalable. Dans le cas contraire, le responsable désigné devra évaluer le bon niveau de remontée, en fonction de l'ampleur de la fraude soupçonnée, de l'organisation et des structures concernées par le soupçon.

© IFACI

4.5- Mesures conservatoires

Dans certaines situations, l'analyse initiale (cf. Partie 4.1, p. 37) peut conduire à décider la mise en œuvre de mesures conservatoires cohérentes avec les dispositions d'investigation retenues.
C'est en particulier le cas dans l'hypothèse où la fraude soupçonnée pourrait avoir des conséquences importantes pour l'organisation, il peut être nécessaire d'envisager des mesures conservatoires, sans attendre les conclusions des investigations. Les mesures envisagées viseront essentiellement à :

- réduire les conséquences de la fraude, dans l'hypothèse où elle serait avérée, en sécurisant des locaux, des accès à des données et à des documents ;
- éviter la reproduction de situations de fraude analogues avant la fin des investigations et la mise en œuvre d'un retour d'expérience approfondi ;
- prendre les mesures de sûreté pour protéger l'organisation (sécurisation des locaux, des documents, des données informatiques) et les parties prenantes (exemple : fraude perpétrée par le crime organisé).

Lorsque le risque d'image est important, la direction de la communication doit systématiquement être associée pour que l'organisation ait une position non ambiguë, validée par la direction générale. En règle générale, un porte parole unique est désigné pour faire l'interface avec les médias.

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

4.6- Phase d'investigation

La phase d'investigation constitue la phase la plus délicate du processus, mais doit être facilitée par toutes les précautions prises auparavant. Ces quelques pages n'ont pas pour vocation de vous expliquer les détails d'une investigation, mais de mettre en avant les principales difficultés que vous risquez de rencontrer.
L'investigation doit se mener selon un plan de travail détaillé qui doit permettre le suivi de la progression et le cadrage des opérations.

4.6.1. Objectifs de la phase d'investigation

Il est important de ne pas se limiter à la recherche d'un fraudeur, mais plutôt de se concentrer sur la recherche de la faille dans le système. C'est la connaissance de ces défaillances qui constitue la plus value pour l'organisation. Elle pourra en tirer les leçons et établir un dossier efficace pour les tribunaux judiciaires et prud'homaux.
Ainsi donc, au-delà de l'identification du ou des fraudeurs potentiels et de leurs modes opératoires s'il y a lieu (objectif à court terme), la phase d'investigation doit permettre de :

- rassembler les preuves et les indices pour une éventuelle poursuite s'il s'avère qu'il y a un fraudeur (objectifs à moyen terme) ou pour disculper les personnes dénoncées sans fondements ;
- qualifier les failles du système et les corrections à apporter (objectif à long terme).

Objectifs	Conséquences
Identification du ou des fraudeurs potentiels	➔ Suppression du risque possible. ➔ Possibilité de procès.
Rassemblement des preuves	➔ Possibilité de récupérer les sommes en jeu. ➔ Possibilité de prendre des mesures disciplinaires justifiées.
Qualification des failles	➔ Protection renforcée de l'organisation sur ces processus. ➔ Identification d'autres cas.

La phase d'investigation se distingue d'une mission classique d'audit interne par deux aspects :

- il n'est pas possible de se contenter de tests de couverture, il faut trouver un indice, voire une preuve.
- ne pas négliger les détails et les montants peu significatifs, ils peuvent mener à des éléments plus importants (exemple : écritures reliées à d'autres écritures) ou s'additionner (fréquence). Ne pas oublier que les fraudeurs savent souvent passer en-dessous des seuils.

© IFACI

4.6.2. Gestion du temps

Les moyens à mettre en œuvre doivent être définis et évalués au départ en se posant deux questions clés :

- Combien de personnes sont affectées à ce dossier (temps passé en nombre de jour/homme) ?
- Combien de temps se donne-t-on pour résoudre le cas (délais) ?

Il faut pouvoir arbitrer entre le fait :

- d'agir vite pour gérer rapidement le problème de confidentialité ;
- de prendre son temps pour avancer prudemment et constituer un dossier solide qui peut être utile pour récupérer des éléments détournés.

Le temps doit être géré en fonction des objectifs définis. Il doit avoir été défini dans la phase de cadrage et être revu au fur et à mesure, dans le cadre des modalités de gestion et de décision qui ont été définies.
La pluralité des intervenants doit également être prise en compte dans la gestion du temps. Elle peut aussi modifier la donne, car l'intervention de spécialistes ou de plusieurs consultants peut accélérer le dossier, s'ils sont bien coordonnés.

4.6.3. Intervenants

Les intervenants sont définis dès le départ et leur implication doit être autorisée par le comité.

Le responsable de l'investigation et l'éventuelle équipe associée sont compétents et n'ont aucun lien présent ou passé avec des suspects identifiés. Ils sont, en principe, indépendants du périmètre d'enquête.
Le responsable de l'investigation est doté des pouvoirs nécessaires pour accéder librement aux informations utiles. Les bonnes pratiques professionnelles des auditeurs internes sur la documentation d'une mission peuvent être utiles. Selon les cas, le recours à une ressource experte interne (informatique, financière, etc.) ou à un enquêteur externe peut être envisagé.
Le responsable de l'investigation veillera à la sauvegarde et à la sécurisation des preuves recueillies (documents, unités de stockage de données informatiques, etc.). Il est responsable du respect de la législation, notamment pour ce qui concerne la loi Informatique et Libertés en France.
Il formalise les scripts préliminaires et mène les interviews nécessaires, de préférence accompagné d'une deuxième personne de confiance, elle aussi indépendante (enquêteur ou représentant de la direction des ressources humaines). Sauf exception, les premières interviews ne concernent pas les suspects directs et en cas de multiples suspects, une approche progressive est recommandée, des moins importants aux plus importants.

© IFACI

En cas de tiers lésés, le responsable de l'investigation interviendra directement ou indirectement pour collecter les informations ou documents nécessaires en toute confidentialité.
Indépendamment des *reportings* réguliers remis au responsable du traitement, un rapport d'investigation final détaillé lui est remis avec les éléments de preuves confirmant (ou infirmant) la fraude supposée. En cas de fraude avérée, les causes et mécanismes sont exposés en détail. Les conclusions de ce rapport permettront la prise des décisions nécessaires.

Tous ces intervenants, qui ont du être identifiés auparavant, doivent signer une clause de confidentialité et communiquer selon des modalités définis.
Il est important de ne pas préjuger de ses capacités et de faire appel à des compétences extérieures en cas de difficultés. Il en va des chances de succès de la conclusion du processus.
Pour toute intervention extérieure, un contact doit exister en interne pour communiquer, gérer et filtrer les informations et discuter les résultats.
On distingue plusieurs groupes :

- les « aides » (experts internes (juridiques, RH), experts externes, contacts externes, forces de l'ordre, Justice) ;
- les « facilitateurs » (responsables techniques (tels que le responsable système informatique)) qui vont permettre d'accéder à l'information en toute sécurité et de manière efficace ;
- les « collaborateurs » (supérieurs hiérarchiques) ;
- les « valideurs » (membres du comité qui vont donner leur accord).

Exemples d'attitudes à éviter :

- Arriver dans le service informatique et demander au premier venu une extraction de données sensibles. La suspicion peut envahir toute l'organisation très vite.
- Laisser faire un consultant extérieur sans lui donner un cadre de travail précis et en le faisant reporter à un dirigeant. Celui-ci ne prendra pas forcément le temps de s'y plonger en détail.

4.6.4. Travaux à réaliser

Le plan des travaux doit être défini à l'avance et les changements doivent être remontés au comité en charge du dossier.
L'investigation peut consister en :

- des analyses classiques de processus (notamment la recherche des failles de type non séparation des tâches), absence de protection (codes) ou de contrôles *(reportings)* ;
- des analyses de documents et de données qui pourraient contenir des éléments à exploiter ;
- une recherche d'indices ou de preuves qui pourraient corroborer des résultats d'analyse ;
- des entretiens avec des témoins (supérieurs, collaborateurs) ;
- des entretiens avec les suspects.

© IFACI

Toutes ces actions peuvent apparaître nécessaires en fonction de l'avancée du dossier. Le comité de suivi doit être informé des actions significatives. Des comptes rendus réguliers peuvent être faits en détaillant les avancées et les actions engagées.

4.6.5. Recherche de document ou de données

Les documents ou données, que vous recherchez, peuvent être de 4 types :

- Données et documents internes à l'organisation – exemples : comptes, données extraites des applications de gestion, relevés d'heures.
- Données mixtes (internes et externes) – exemples : bon de livraison validé par un client, réponse d'un tiers à un mail interne.
- Données et documents externes – exemples : documents d'organisation (actionnariat dans le cadre d'un conflit d'intérêt).
- Données et documents personnels du suspect, dans le respect de la règlementation en vigueur – exemples : mèls, courriers, notes, brouillons.

4.6.6. Entretiens

Les entretiens peuvent se mener dans deux situations :

- Etude générale des processus et recherche d'explications.
- Mise à l'épreuve ou confrontation du suspect.

Dans le 2ème cas, il conviendra de respecter le droit du salarié. Cet entretien doit se mener dans des conditions particulières et avec une grande prudence.
Les entretiens servent à étudier le cas et à prendre d'éventuelles mesures disciplinaires. Ce ne sont pas des preuves légales directement utilisables dans le cadre d'une procédure judiciaire.

Point de vigilance juridique : Droit de la preuve

Une entreprise peut être selon le cas auteur ou victime d'une fraude. En droit français, il existe, deux systèmes de preuve qui se distinguent de la manière suivante :

- d'une part, les moyens de preuve préalablement déterminés et imposés par loi. C'est ce que l'on appelle la preuve dite « légale ».
- d'autre part, les moyens de preuve libre, sans détermination ni exigences légales ou réglementaires.

C'est ce dernier système qui s'applique aux faits juridiques relatifs à la fraude, en particulier dans le domaine de la fraude informatique. Ainsi, suivant les termes de l'article 427 du Code de procédure pénale : *« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve […] ».*

© IFACI

Il s'agit principalement de rapporter la preuve de **l'élément matériel de la fraude.** A cet effet, en matière de fraude informatique toutes les données enregistrées sur le système sont recevables devant la justice, pourvu que celles-ci respectent (i) les droits de la vie privée sur les données à caractère personnel et (ii) les droits de la défense (principe du contradictoire).

Attention : l'utilisation de « pièges à fraudeurs » fondés sur des procédés illicites ou déloyaux est à éviter. Par exemple, lorsque l'entreprise tente d'intercepter des correspondances ou des échanges par méls, il faut qu'elle respecte l'exception de confidentialité et du respect de la vie privée qui s'impose notamment sur les espaces et répertoires personnels des salariés. En effet, ces espaces constituent le domicile virtuel de la personne privée. Ils ne peuvent être interceptés, même si ce domicile virtuel est implanté sur le système informatique professionnel de l'entreprise.

La recevabilité des preuves informatiques est donc cruciale. En pratique, il est indispensable de prendre toutes les précautions juridiques et techniques préalables pour la capture, la conservation et l'analyse des données susceptibles d'être présentées en justice.
L'entreprise doit avoir une approche proactive et anticiper la mise en place de règles et procédures de capture, de conservation et d'analyse des données professionnelles en les distinguant des données personnelles.
Il est indispensable d'actualiser ces règles et procédures au fur et à mesure des avancées jurisprudentielles[1].
Ces règles et procédures internes auront pour objet principal de permettre de rapporter la preuve pertinente : (i) du **caractère intentionnel** de l'accès frauduleux ou de l'utilisation frauduleuse du système d'information, (ii) d'**identifier l'auteur ou de rendre imputable** à une ou plusieurs personnes la commission de l'infraction.

4.6.7 Précautions à prendre

Les travaux d'investigation doivent être documentés et référencés pour pouvoir être ensuite utilisés lors des entretiens, lors d'un procès. Vous devrez faire attention à ne pas altérer les documents et fichiers originaux pour qu'ils puissent être reconnus comme preuve. La direction juridique devra vous aider sur ce point.
Dans beaucoup de cas, l'investigation va consister à cibler des anomalies dans les systèmes informatiques et à récupérer les preuves matérielles (documents signés, par exemple), c'est cette dernière phase qui sera délicate.
L'établissement d'un cadre de travail et l'identification préalables des interlocuteurs (Ressources Humaines, Juridique) sont indispensables pour mener à bien l'investigation, en respectant le droit

[1] *S'agissant des SMS, un arrêt de la chambre sociale de la Cour de cassation a jugé que l'utilisation d'un SMS comme mode de preuve était un procédé loyal recevable, par opposition à l'enregistrement d'une conversation téléphonique privée effectuée à l'insu de son auteur, car ce dernier ne peut ignorer que les messages sont enregistrés par l'appareil récepteur (Cass. soc., 23 mai 2007).*

© IFACI

social et les règles légales. Le cas échéant, ces résultats pourront être utilisés dans le cadre d'une action en justice et mener à une condamnation du suspect.
La Commission Nationale de l'Informatique et des Libertés (CNIL) encadre les conditions d'une investigation, notamment en :

- définissant les conditions d'accès aux informations personnelles (mails) ;
- définissant les conditions de surveillance (caméras, écoute) ;
- garantissant la confidentialité et la sécurité des investigations, en limitant les possibilités de rassembler et garder des informations sur les personnes, sous forme de listes nominatives, et en exigeant une sécurité et une confidentialité pour ces données.

A éviter :

- Prendre des décisions disciplinaires contre les personnes soupçonnées, sans s'assurer de leur conformité aux exigences du droit social, ni gérer le risque de contentieux devant les prud'hommes.
- Fouiller les locaux sans précaution et obtenir des preuves de manière irrégulière.

Cf. Points de vigilance juridique : « droit de la preuve » p.54 et « fraude et droit pénal » p. 57.

4.6.8. Analyse comportementale

L'aspect investigation comporte plusieurs phases qui, même si elles sont aujourd'hui vulgarisées par les médias, ne sont pas à la portée de tout le monde.
Ne vous lancez pas dans une analyse comportementale si vous n'en avez pas la compétence. Si certains signes peuvent trahir une personne, rien n'est évident. Une voiture de sport ou une addiction au jeu ne sont pas des preuves tangibles, il peut toujours exister des explications.
Néanmoins, il est utile de prendre en compte des changements de comportement ou des événements familiaux, professionnels pour pouvoir cibler une motivation ou une rationalisation. D'autre part, des signes pratiques comme, par exemple, l'absence de prises de vacances, des refus catégoriques ou la réalisation de tâche mineure par rapport à un niveau hiérarchique peuvent être liés à une peur d'être démasqué lors d'une absence ou d'une délégation.
Lors des entretiens, il convient d'être attentif aux réponses et aux réactions. Cependant, l'analyse comportementale ne s'improvise pas. C'est une véritable expertise qui permet de mettre à jour des incohérences dans les réponses et d'aboutir à un aveu.
Enfin, à l'instar d'un profileur, il est utile de se mettre dans la peau d'un fraudeur pour imaginer quels types de fraude il a pu commettre. Pour identifier les failles, il faut arriver à se démarquer des schémas classiques pour se mettre en situation et imaginer différents scénarii. L'intérêt de cette méthode est de s'adapter à la situation, car chaque cas est unique, plutôt que de plaquer des scénarii classiques.
Ces méthodes peuvent être utiles, mais sont à utiliser avec modération et ne permettent pas de conclure.

© IFACI

4.6.9. Investigation judiciaire

Le recours en justice peut faire partie du processus d'investigation. Cette décision résultera d'une concertation avec la direction juridique qui décidera de la méthode et de la procédure à adopter (cf. Partie 4.7, p. 59). Néanmoins, le responsable de l'investigation a un rôle capital dans ce processus puisque la procédure reposera sur son travail. Sa responsabilité peut être mise en cause en cas d'échec, voire de poursuite en diffamation de la part du suspect.
Le dossier devra être clair et pédagogique car les autorités judiciaires ne maîtrisent pas forcément les enjeux liés au métier et à la structure de l'organisation.

Le recours en justice peut permettre de faire avancer l'enquête en permettant, notamment, des perquisitions ou des interrogatoires. Il ne signifie pas que l'investigation interne est terminée.

Point de vigilance juridique : Fraude et droit pénal

La fraude n'est pas définie en tant que telle dans le Code Pénal français. Elle comprend différents actes dont certains sont sanctionnés par le code pénal. Par exemple :

- Escroquerie (article 313-1 du Code Pénal).
- Faux (article 441-1 du Code Pénal).
- Abus de confiance (article 314-1 du Code Pénal).
- Vol (article 311-1 du Code Pénal)
- Atteinte aux systèmes de traitement automatisé de données (article 323-1 et suivants du Code Pénal), etc.

La question de la qualification juridique est l'un des nombreux écueils rencontrés lorsque des faits frauduleux sont dénoncés auprès des services de police, du procureur de la république ou du doyen des juges d'instruction.

La saisine des personnes susvisées déclenche alors l'action publique, qui a pour objectif de mettre fin à l'infraction et sanctionner l'atteinte qui est faite aux lois de la République, mais cette saisine peut également s'avérer problématique.

Par ailleurs, l'action pénale n'a pas pour objet de réparer le préjudice subi par la société. Pour ce faire, cette dernière doit se constituer « partie civile » pour réclamer auprès de la juridiction compétente la condamnation du prévenu à lui réparer son entier préjudice.
L'examen du préjudice de la société peut se faire lors du procès pénal, selon des règles bien précises.

Bien que l'intervention d'un avocat ne soit pas obligatoire dans ce type de procédure, il est cependant fortement recommandé de recourir à un tel conseil pour maîtriser la complexité des règles de

© IFACI

procédure. Le recours à un avocat permet de gagner du temps et d'obtenir son assistance technique sur tous les aspects du dossier : formalisation de la plainte, constitution de partie civile, suivi de la procédure (assistance éventuelle devant le juge d'instruction, obtention de la copie du dossier pénal, demandes complémentaires), plaidoirie, suivi de l'exécution du jugement, etc.

© IFACI

4.7- Conclusion

4.7.1. Comment préparer la conclusion ?

Selon le degré d'urgence, il faut établir un rapport qui tient compte des priorités.

Le rapport doit contenir :

- les principes de la fraude ;
- les éléments de preuve à charge et à décharge ;
- les actions internes à mener, à détailler plus ou moins en fonction de l'urgence de sortir le dossier ;
- les conclusions sur la base du rapport.

Les décisions nécessaires à la bonne préservation des intérêts de l'organisation concernent, notamment :

- la mise en œuvre des procédures de sanctions disciplinaires contre les auteurs de la fraude (salariés, mandataires, délégataires, etc.) ;
- le contrôle des biens professionnels utilisés par ceux-ci (données, outils, etc.). La suppression des accès physiques et logiques, la restitution des objets (badges, clés, véhicule, PC, téléphonie, etc.) ;
- l'information des personnes externes ou internes à l'organisation, potentiellement lésées (clients, partenaires d'affaire, etc.). Cette information est plus ou moins exhaustive (a minima, il s'agira d'indiquer un changement d'interlocuteur). Elle pourra nécessiter un rendez-vous, en coordination avec la direction de la communication.

C'est à la direction générale de décider comment gérer la fin de ce dossier.

Jusqu'à la décision formelle de clôture par l'organisation, un cas reste suivi, même en veille. Il fait l'objet d'un reporting ad hoc. En cas de poursuites judicaires ou de contentieux, le cas peut durer plusieurs années, des points d'étapes sont formalisés afin de ne pas perdre des opportunités de défendre au mieux les intérêts de l'organisation (par exemple : date butoir pour se porter partie civile).

4.7.2. Prise de décision

La décision de clôture d'un cas de fraude avérée doit intervenir lorsque toutes les mesures raisonnables de préservation des intérêts de l'organisation ont été prises et que les possibilités de réparation du préjudice ont été épuisées.

© IFACI

Il est temps de conclure et de prendre une position quand :

- la fraude est avérée ;
- le soupçon est infondé ;
- le soupçon n'est pas dissipé.

La clôture peut également être justifiée par l'impossibilité de prouver la fraude ou si la déclaration initiale de faits potentiellement frauduleux s'avère non fondée.
La décision de clôture est actée formellement. L'archivage doit respecter la loi informatique et libertés (droit à l'oubli).

Il ne faut pas craindre de ne pouvoir conclure. Par exemple, on accuse des managers d'accorder des congés non justifiés à leurs équipes, mais il n'est pas possible de prouver que les personnes n'étaient pas présentes.
Cette possibilité doit être prise en compte par la direction générale car une accusation à tort peut porter préjudice, voire entraîner des poursuites.

Sur le plan judiciaire, en fonction de la politique de l'organisation, le responsable du traitement coordonne, avec la direction juridique, le recours à un conseil extérieur (avocat) et la mise en œuvre de poursuites judiciaires.

4.7.3. Agir en conséquence

Si la fraude est avérée, il peut être fait appel à la justice, soit pour prendre la main jusqu'au procès, soit pour renforcer le dossier en donnant un accès plus large aux autorités judiciaires dans le domaine de la recherche des preuves. (cf. Point de vigilance juridique : Droit de la preuve, p. 54).
Dans le même temps, le processus disciplinaire sera lancé par la direction des ressources humaines. L'organisation adaptera sa communication interne à la priorité qu'elle veut donner à ce sujet.

Point de vigilance juridique : Fraude et droit du travail

La découverte de la fraude et la prise de sanctions à l'encontre de son auteur doivent être conformes aux exigences posées par le droit du travail.

On peut en distinguer au moins deux :

- Premièrement, la mise en place de canaux d'information pour détecter les cas de fraude ne doit pas apporter de restrictions disproportionnées aux droits et libertés des salariés.
  Ceux-ci doivent être informés des moyens de contrôle mis en place, tels qu'une ligne « éthique » aussi appelée hotline ou *Whistleblowing*, destinée à inciter les salariés à signaler les comportements fautifs de leurs collègues ou des dirigeants de l'organisation, susceptibles de nuire à celle-ci ou d'engager sa responsabilité. Faute de les avoir informés, l'employeur ne saurait reprocher aux salariés un manquement à leurs obligations et, par voie de conséquence, les sanctionner.
- Deuxièmement, l'auteur d'une fraude peut faire l'objet de sanctions disciplinaires, allant de l'avertissement au licenciement. Toutefois, la prise de sanctions doit respecter les règles du droit disciplinaire, posées par le droit du travail (loi, convention collective, règlement intérieur) protectrices des droits des salariés.

Ainsi, par exemple, un licenciement justifié par une fraude (licenciement disciplinaire) devra obligatoirement être précédé d'un entretien préalable. Lorsque la fraude invoquée est constitutive d'une faute grave, la procédure disciplinaire doit être engagée rapidement contre le salarié, à défaut de quoi elle sera irrégulière. Toutefois, si une enquête est nécessaire pour caractériser les faits frauduleux, la procédure pourra être engagée à l'issue de cette enquête, pendant laquelle le salarié pourra avoir été écarté de l'organisation, via une mise à pied conservatoire.

Les actions en justice et le processus disciplinaire devront également être suivis par la direction de la communication externe. En effet, elle devra traiter les éventuelles informations parues dans la presse et gérer les informations et déclarations de l'organisation.
Si le soupçon est infondé, il faut savoir gérer la fin du dossier en refermant tous les dossiers afin d'éviter les fuites qui pourraient perturber la vie de l'organisation.
Si le soupçon n'est pas dissipé, il faut mettre en place des systèmes de veille, dans le respect des réglementations, afin de pouvoir continuer à surveiller ces processus. Il faut songer, avant tout, à renforcer les contrôles et le faire savoir, via de nouvelles procédures.

4.7.4. Gérer les conséquences

Le rapport sur la fraude sera complété par un rapport plus détaillé sur les actions à mettre en œuvre (après l'application des mesures conservatoires d'urgence) pour modifier les processus, l'organisation ou les systèmes d'information. Ce rapport pourra donner lieu à une communication de crise restreinte, destinée à informer l'encadrement des dangers potentiels.
La direction comptable doit être informée des éléments chiffrés permettant la comptabilisation (pertes, provisions) du cas.
Dans le cadre de la politique de fraude, il est nécessaire de prendre le temps de considérer et de valoriser le discernement et la perspicacité des personnes qui ont œuvré utilement dans le cadre de la procédure.

© IFACI
© IFACI

© IFACI

Partie 5

Un outil de prévention et d'anticipation : la cartographie des risques de fraude

La fraude est un risque majeur pour tous les types d'organisation. Il peut être évalué dans le cadre des démarches globales de cartographie des risques. Cependant, compte tenu du caractère polymorphe des faits générateurs de la fraude (cf. partie I sur le triangle de la fraude) et de ses différents impacts, la représentation du risque de fraude dans la cartographie globale des risques majeurs n'est pas suffisante. En effet, une approche spécifique sera nécessaire pour que tous les bénéfices de cet outil soient utilisés comme levier du dispositif de pilotage et de prévention du risque de fraude.

Cette partie du cahier de la recherche illustre la démarche classique d'élaboration d'une cartographie mais elle ne la détaille pas. Pour connaître les principes généraux de la cartographie des risques, veuillez vous référer aux documents de référence sur le sujet.

Bibliographie sur le management des risques et la cartographie des risques :

- Le management des risques de l'organisation – COSO II report.
- Le dispositif de gestion des risques et de contrôle interne / Cadre de référence – AMF.

Le risque de fraude n'est pas un risque comme un autre. Il a des spécificités liées à :

- son caractère particulièrement aléatoire ;
- sa dissimulation ;
- sa rationalisation ;
- la difficulté d'évaluer l'impact du risque d'image ;
- l'effet domino ;
- la tendance à le sous-estimer, etc.

© IFACI

© IFACI

5.1- Objectifs de la cartographie des risques de fraude

La cartographie est l'outil d'aide au calibrage et au pilotage du dispositif de lutte contre la fraude. Le niveau d'analyse des risques devra donc être adapté aux objectifs, au périmètre et aux moyens du dispositif.

La cartographie permet de :

- mieux appréhender les différentes composantes du risque de fraude et leur niveau de criticité ;
- fournir une vision d'ensemble du risque de fraude au sein de l'organisation ;
- cibler des activités ou des domaines du périmètre de responsabilité de l'organisation. Elle peut être utilisée pour la structuration du dispositif de gestion des risques ;
- donner au management et aux instances de gouvernance une appréciation du niveau d'exposition au risque de fraude ;
- apporter un des éléments de réponse à la question du suivi de l'efficacité du dispositif de contrôle interne et de gestion des risques prévu par l'ordonnance du 8 décembre 2009 (transposition de la 8ème directive européenne) ;
- d'anticiper et d'aller au-delà d'une analyse des cas détectés ou de certains éléments remontés à travers un dispositif d'alerte professionnelle (type *Whistleblowing*) ;
- identifier les actions prioritaires à mettre en œuvre.

© IFACI

5.2- Les étapes de l'élaboration de la cartographie des risques de fraude

L'élaboration de la cartographie des risques de fraude est modulable selon des éléments de contexte tels que :

- les destinataires de la cartographie ;
- le niveau final d'agrégation (au niveau d'une entité ou au niveau du groupe) ;
- la ventilation éventuelle selon les processus majeurs, les branches d'activité, les zones géographiques, etc. ;
- l'homogénéité des processus entre les différentes filiales ou zones géographiques ;
- les autres démarches de cartographie et/ou d'auto-évaluation des risques ;
- la maturité du dispositif de lutte contre la fraude (cf. Partie 2 p. 19 et Partie 3.3 p. 27).

L'approche doit être proportionnée aux enjeux et au contexte :

- s'appuyer sur les dispositifs existants (cf. Partie 2 p. 19 et Partie 3.3 p. 27) ;
- tenir compte du rôle des acteurs clés tels que le Conseil d'administration, la direction générale, le Comité d'audit, le gestionnaire des risques, l'audit interne, le juridique, la DSI, la direction opérationnelle, etc. (cf. Partie 2 p. 19 et Partie 3.3 p. 27).

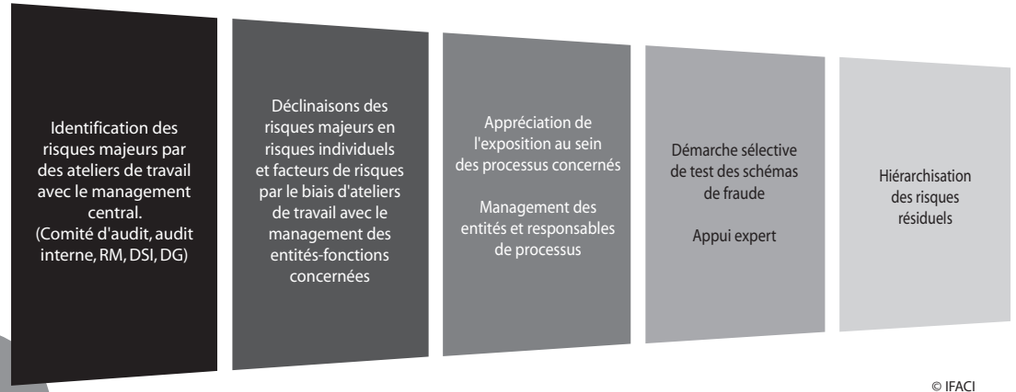
L'exhaustivité est impossible à atteindre surtout sur un sujet comme le risque de fraude :

- privilégier le niveau de criticité en identifiant les 10 ou 15 principaux risques ;
- si une approche par activité ou par processus est retenue, cibler les domaines à enjeux.

5.2.1. Définir une approche

Selon les objectifs poursuivis par l'organisation et le niveau de granularité recherché, deux types d'approches peuvent servir à construire la cartographie :

L'approche top-down :



© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

L'approche *top-down* part de risques majeurs identifiés au niveau le plus élevé de l'organisation pour ensuite analyser leur niveau de criticité pour une activité, une zone géographique, un processus donnés. Cette démarche est particulièrement efficace pour évaluer les risques majeurs de fraude qui empêcherait la réalisation des objectifs de l'organisation.

L'approche bottom-up :

Avec l'approche *bottom-up*, les risques spécifiques sont d'abord identifiés par les propriétaires de processus ou les responsables d'activité. Elle bénéficie de leur connaissance métier. L'identification des risques peut être structurée en utilisant une liste non hiérarchisée des risques. Elle peut résulter d'une analyse du niveau d'exposition au risque de fraude du secteur d'activité et des faiblesses de l'organisation (cf. Partie 2, p. 19). Cette démarche est directement déployée par des services dédiés à la réalisation de la cartographie et/ou dans le cadre d'une auto-évaluation réalisée par les responsables d'entités.

- L'ensemble de l'organisation doit être au courant de la démarche. Cette mise sous tension a mécaniquement un rôle de prévention.
- Même si la fraude ne doit pas rester taboue, l'analyse du risque de fraude demeure sensible. Le partage des techniques d'analyse des risques de fraude se limite, de préférence, à certains interlocuteurs.
- L'auto-évaluation du risque de fraude est à mettre en œuvre dans des organisations qui ont un bon niveau de maturité. Les acteurs de l'auto-évaluation devront être sensibilisés aux caractéristiques de la fraude (cf. Partie 1.1, p. 11). Une évaluation indépendante de cette démarche permettra également de limiter le risque d'instrumentalisation.
- L'intégration dans des démarches globales d'auto-évaluation des risques pourra être envisagée. Elle permet la sensibilisation d'un grand nombre de collaborateurs et pourra être complétée par des analyses ciblées.
- Le choix des domaines où ce type d'approche doit être déployé est d'abord lié aux enjeux sous-jacents. Sans pour autant perdre de vue le fait que la fraude, risque «caché» par essence, peut être perpétrée hors des processus « cœur de métier » ou à fort enjeu financier.
- La prise en compte d'éléments factuels provenant, par exemple, de bases incidents ou d'indicateurs de défaillance du contrôle interne
- La nécessité de consolider un nombre important de risques de fraude dispersés sur l'ensemble du périmètre de l'organisation constitue une des limites de l'approche *bottom-up*.
- L'accompagnement de l'approche *bottom-up* et le traitement de l'information obtenue engendrent ainsi un travail conséquent qu'il convient d'organiser en amont pour réduire la perturbation occasionnée et obtenir une participation satisfaisante.

Les deux approches ne sont pas exclusives. Ainsi, l'analyse *bottom-up* pourra être mise en perspective avec les risques majeurs identifiés à travers une démarche *top-down*. A chaque fois que cela est possible, il convient d'exploiter les avantages de chaque approche car elles sont complémentaires :

© IFACI

- l'approche *top-down* a l'avantage de la cohérence et de l'anticipation ;
- les démarches *bottom-up* sont un excellent moyen de capitalisation. Leur caractère opérationnel les rend particulièrement utiles pour les métiers.

Glossaire

- Un **risque inhérent (brut)** est le risque avant la prise en compte des mesures de contrôle et d'assurance. L'analyse des risques opérationnels se fait généralement par la notion de risque brut, de façon à identifier quel mode de traitement a été mise en place. (cf. Le management des risques de l'entreprise – COSO II Report, p. 204).
- Le **risque net (résiduel)** quant à lui subsiste malgré les mesures de contrôle, de prévention et d'assurance ont été prises (cf. Le management des risques de l'entreprise – COSO II Report, p. 205, cf. Glossaire, le cadre de référence international des pratiques professionnelles de l'audit interne, IIA/IFACI). Il est accepté par les instances dirigeantes.
- Selon la définition des normes ISO (ISO/CEI 51-73), le terme « mesures de prévention » est, ici, à prendre au sens de l'ensemble des mesures permettant de réduire le risque à la source. (cf. Le management des risques de l'entreprise – COSO II Report, encadré p. 230, les 4 types de mesure de traitement : éviter, partager, réduire, accepter).
- La **criticité d'un risque** est définie comme facteur de vraisemblance donnant une intensité plus ou moins grande au risque . Selon les méthodologies employées, la criticité peut être le produit de la probabilité par l'impact du risque (autre nom pour l'« espérance », terme mathématique).
- Un **risque majeur** est la possibilité qu'un événement, dont les effets peuvent mettre en jeu un grand nombre de personnes, puisse générer des dommages jugés importants aux yeux d'une organisation. Il peut être jugé majeur du fait de son haut niveau de criticité (cf. Annexe 1, p. 84).
- Un **risque significatif** est un risque dont l'impact pourrait modifier les décisions économiques ou l'appréciation portée sur les comptes. Le seuil de significativité du risque relève du jugement de l'organisation. Il est fondé sur des critères pertinents tels que l'effet sur le résultat courant, le résultat net, le chiffre d'affaires, etc.

5.2.2. Identifier les risques majeurs inhérents

Cette identification peut être structurée selon :

- la typologie de fraude définie dans l'organisation (cf. Partie 1.2, p. 14) ;
- les composantes de l'organisation pouvant être affectées ;
- les objectifs de l'organisation.

© IFACI

Les objectifs définis dans des référentiels, tels que le COSO II ou le cadre de référence de l'AMF, peuvent constituer des axes d'identification des risques de fraude au niveau :

- Stratégique ;
- Opérationnel ;
- *Reporting* ;
- Conformité.

La composante informatique est transverse à ces quatre dimensions. Elle doit constituer un point de vigilance particulier en ce qui concerne le risque de fraude.

Plusieurs méthodologies d'identification des risques coexistent et sont complémentaires. Elles sont récapitulées dans le tableau ci-dessous :

Utilisation de bases de données réelles	➔ Dans une organisation donnée, le nombre de cas avérés de fraude n'est par toujours suffisant pour permettre une analyse statistique de corrélation ou de projection. ➔ En revanche, la remontée d'informations à partir de bases d'incidents ou d'indicateurs de fraude potentielle constitue une masse de données susceptible de faire l'objet d'une analyse statistique. Elle peut également être utilisée pour construire des modules de détections d'anomalies sur d'autres bases de données (type ERP).
Ateliers d'auto-évaluation	➔ Une fois les premières identifications effectuées, il est possible de proposer une liste des risques identifiés à partir de cas avérés (cf. annexe 5, p. 108) ou d'autres sources d'informations (par exemple, rapport d'audit). ➔ Les risques recensés sont ensuite analysés collectivement pour déterminer leur impact pour l'organisation et la qualité des mécanismes de couverture (par exemple, conception, existence, contrôle). ➔ Une session de synthèse clôture l'atelier avant discussion et validation avec le management.
Envoi de questionnaires	➔ Réunir, pour un atelier, l'ensemble des acteurs clés à associer à la démarche de cartographie du risque de fraude peut s'avérer difficile. Le questionnaire peut alors s'utiliser de façon complémentaire ou être construit sur la base des entretiens menés auparavant. ➔ La rédaction des questionnaires demande une attention particulière à plusieurs niveaux : • Le contrôle de leur diffusion. A nouveau, la fraude ne doit pas rester taboue mais elle demeure un sujet sensible en évitant de préférence de fournir trop de clés de fraude aux fraudeurs potentiels • La qualité de rédaction des questions. Le sens des questions peut bien évidemment orienter les réponses. Il faut éviter l'auto-censure. • La véracité des réponses et de l'identité de la personne qui a répondu. • La qualité des réponses est parfois difficile à appréhender (la personne a-t-elle répondu hâtivement ?).

© IFACI

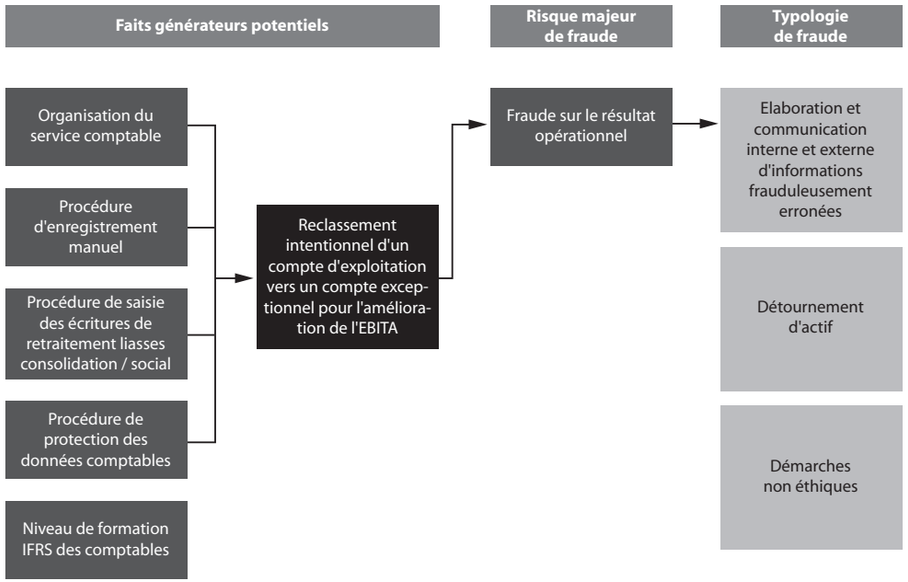
Benchmarks internes et externes	➔ Une proportion importante des cas concerne des fraudes très similaires. Par exemple, l'affaire Madoff correspond à un schéma de fraude utilisé par Charles Ponzi en 1921. ➔ L'échange entre direction de l'audit, départements dédiés, services de gestion des risques et autres, peut enrichir l'analyse. ➔ Dans un groupe, les leçons tirées de cas détectés dans d'autres branches doivent être mutualisées.

5.2.3. Identifier les faits générateurs et les conséquences des risques

Pour être pertinente, **l'analyse des risques majeurs de fraude doit porter sur l'ensemble des causes pouvant être à l'origine du risque** (concept d'arbre de cause à effet). Cette démarche facilitera la conception et la réalisation des différentes mesures de traitement qui réduiront le risque inhérent à un niveau résiduel acceptable par la direction générale.
La documentation de cette analyse doit être préparée et rigoureuse. Pour structurer la démarche, il est recommandé de passer en revue les axes du triangle de la fraude :

- les éléments d'incitation/pression qui peuvent favoriser la survenance du risque étudié ;
- l'aptitude à rationaliser l'acte ou à l'autojustification ;
- les circonstances qui donnent l'opportunité de commettre une fraude, notamment en fonction de l'environnement de contrôle de l'organisation, du site. (cf. Partie 1.3, p. 14)

Exemple de visualisation des faits générateurs pour un risque donné :



© IFACI

5.2.4. Déterminer le niveau des risques inhérents de fraude et le niveau des risques nets perçus

L'évaluation du niveau de risque inhérent s'effectue en appréciant les résultats précédents selon les deux axes classiques de l'évaluation des risques :

L'impact

Les risques de fraudes sont à considérer comme ayant un impact :

- financier ;
- d'image de l'organisation ;
- lié à la responsabilité des dirigeants ;
- réglementaire ;
- sur le climat interne ;
- effet domino / risque systémique.

Echelle d'impact : l'impact peut être effectivement exprimé en fonction des sommes monétaires en jeu et/ou selon l'atteinte qui peut être portée à l'image ou à la notoriété de l'organisation. Les échelles doivent être de préférence simples, avec un nombre de graduation limité.

La probabilité

Echelles relatives à la notion de probabilité
Ces deux critères permettent de déterminer le **degré de criticité** du risque inhérent :

- majeur ;
- mineur ;
- autres, etc.

Le niveau de criticité est à rapprocher de l'échelle des valeurs de l'organisation (certaines organisations ne définissent pas de seuil de matérialité, systématisent la détection de la fraude quelque soit son niveau).

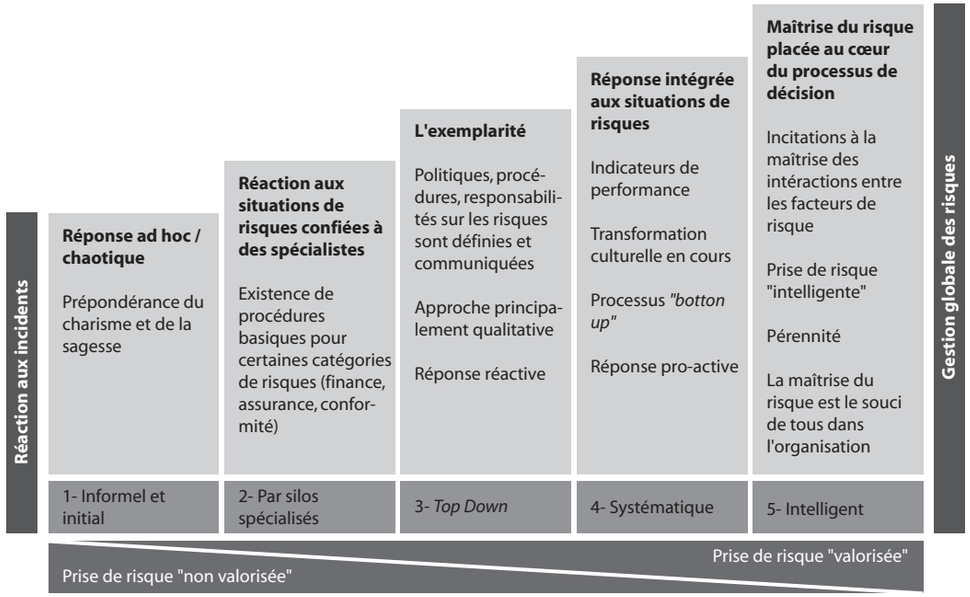
L'évaluation du risque net perçu passe par l'analyse du niveau de maîtrise du risque inhérent. Elle peut, par exemple, être structurée en évaluant les éléments correspondant à l'axe « opportunité » du triangle de la fraude. Par exemple :

- la sécurité physique ;
- les procédures, les activités de contrôle manuelles ou informatisées ;
- la séparation des tâches au niveau organisationnel et systèmes.

© IFACI

Une urbanisation[1] efficace des fonctions de contrôle et de maîtrise des risques constitue un atout pour une bonne évaluation du risque de fraude. En effet, le niveau de maîtrise dépend des données complémentaires remontées par les différents acteurs du dispositif :

- le responsable du site/entité concerné(e) ;
- le responsable financier de l'entité concernée ;
- la fonction contrôle interne / conformité ;
- la fonction d'audit interne ;
- etc.



Le schéma ci-dessus représente les différents niveaux de maturité des dispositifs de gestion des risques. Plus le dispositif de gestion des risques sera mature, plus il sera facile de considérer une intervention interne pour l'analyse du niveau de maîtrise des risques individuels de fraude.

Niveau de risque net perçu = Impact x Vulnérabilité
Sachant que la vulnérabilité = Probabilité x Niveau de maîtrise
Autrement dit, la vulnérabilité correspond à la probabilité que le risque survienne, minorée par les éléments de maîtrise du risque.

Par exemple, la probabilité est notée comme ayant un niveau de 2 sur une échelle de 5. Le niveau de maîtrise, apporté par le système d'information, la séparation des tâches et les autres activités de contrôle manuels et de supervision, est de 4 sur une échelle de 5. La probabilité est réduite de 2 à une vulnérabilité de 1 sur 5.

[1] *L'urbanisme du contrôle interne - Prise de position IFACI, 2008.*

© IFACI

Définition de plans d'actions

La hiérarchisation des risques nets permet de définir des plans d'actions en fonction des différents niveaux de risques perçus.

- **Pour les risques nets perçus comme forts, le plan d'action comprend entre autres :**
  - la sensibilisation des opérationnels et des managers sur le niveau de criticité d'un risque donné ;
  - la mise en œuvre de mesures d'amélioration du niveau de maîtrise de ces risques, tels que la séparation des tâches, les procédures et le contrôle interne ;
  - la mise en place ou le développement d'indicateurs de détection de fraudes potentielles sur ces risques identifiés.

- **Pour les risques perçus comme faible, un contrôle de l'auto-évaluation demeure important.**

5.2.5. Evaluation indépendante du niveau d'exposition

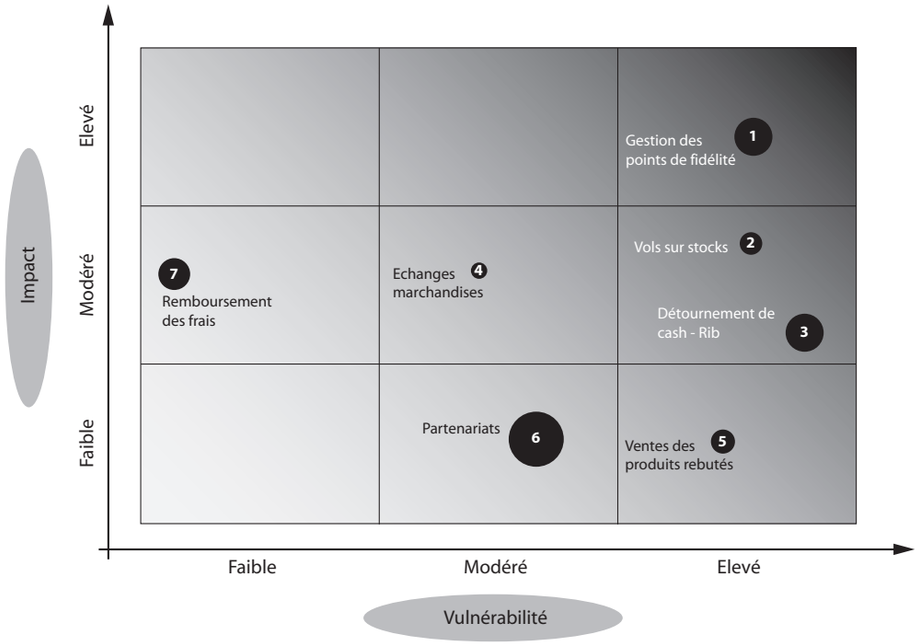
Ce contrôle permet de confirmer la fiabilité des appréciations menées qu'il s'agisse du niveau d'impact ou du niveau de maîtrise.
D'autre part, notre expérience nous amène à considérer que l'analyse des risques de fraude et des différents schémas de fraude n'est pas un exercice qui doit être confié, par exemple, uniquement à un service d'audit interne. La fraude, comme nous l'avons vu, requiert une approche spécifique. Les schémas de fraude sont nombreux et parfois complexes. Dans le cadre d'une analyse du niveau de maîtrise des risques de fraude, les acteurs concernés peuvent être rapidement tentés d'orienter leurs travaux dans la direction d'une investigation. Comme exposé dans ce cahier de recherche, l'investigation fait appel également à des compétences particulières.
Par ailleurs, un nombre de schémas de fraude se répètent selon le secteur d'activité et les typologies de fraude concernées. Un appui expert permet de bénéficier de sa connaissance des schémas de fraudes parfois complexes et des bases de données de schémas utilisées par la profession. L'esprit d'une fraude est particulier, l'analyse du risque associé peut l'être aussi.

© IFACI

5.3- Synthèse et démarche de suivi

5.3.1. Synthèse des travaux

La synthèse des travaux liés à la cartographie du risque de fraude s'inscrit dans un suivi du dispositif de lutte contre la fraude. La synthèse des travaux doit permettre de comprendre le périmètre traité, les acteurs qui ont été impliqués dans la démarche, les composantes du risque de fraude et le niveau d'exposition de l'organisation.
Plusieurs représentations graphiques sont possibles. Un exemple fréquent est le suivant :



La taille des ronds est proportionnelle à la réduction du risque inhérent à un risque résiduel par le biais du niveau de maîtrise dont dispose l'organisation. Plus la taille du rond est petite, plus le niveau de maîtrise est élevé.

© IFACI

5.3.2. Démarche de suivi de la cartographie des risques

La cartographie du risque de fraude doit aller au-delà du simple positionnement de chaque risque dans un diagramme et doit permettre de suivre chaque risque majeur et le fait générateur associé.
Le suivi peut se traduire par exemple par le biais des actions suivantes :

- Tests sur les contrôles forts (cf. cahier de la recherche « l'audit de la fraude dans le secteur bancaire et financier », partie 4.3 - les différents niveaux de contrôle).
- Suivi des incidents et indicateurs.
- Intégration à la démarche de gestion globale des risques avec des reportings trimestriels au comité d'audit / management.

© IFACI

© IFACI

Partie 6

Capitaliser l'expérience à partir des cas avérés

Les types de fraude et le profil des fraudeurs sont très variés. Malgré l'inventivité des fraudeurs, certains mécanismes sont récurrents (par exemple, Madoff = Ponzi). Il convient donc de formaliser l'analyse des cas avérés pour tirer les leçons de l'expérience.

Le modèle ci-après pourra vous servir de base. Il est illustré en annexe 5 (p. 108). Adapté à votre organisation et rempli systématiquement, ce type de fiche contribuera au renforcement des dispositifs anti-fraude (prévention, dissuasion, détection, etc.) présentés dans les autres parties du cahier.

© IFACI

© IFACI

Fiche d'analyse d'un cas de fraude détecté / Titre de la fiche

Fiche n° :

Classification :
- ❑ Fraude interne
- ❑ Fraude externe

Type de fraude :

Canal de détection :

(Préciser la source à l'origine de la détection ➔ exemple : réclamation client, contrôle opérationnel, contrôle interne, audit, dispositif d'alerte professionnelle, tiers…)

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant /Manager
- ❑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :……

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :

(Explication synthétique du déroulement de la fraude)

Evénement générateur - Causes - Défaillances :

(Identification du fait générateur, des causes et des défaillances à l'origine de la fraude- Partir du triangle de la fraude)

Facteurs aggravants de risques détectés :
- ❑ oui
- ❑ non

Si oui, nature du facteur aggravant :

(Exemple : facteurs d'environnement augmentant le risque de survenance de la fraude, défaut ou absence de procédure, modification d'une organisation, insuffisance du contrôle interne…)

© IFACI

Catégorie de fraude[1] :

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ❑ Moyen
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :

- ❑ Pertes financières,
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

Evaluation financière, si pertinente :

Perte brute : .....

% récupéré : .....

Perte nette : .....

Charges d'investigation : .....

Mesures correctrices envisagées : *(Exemple : modification d'un processus, actualisation du dispositif de contrôle a priori et/ou a posteriori, actualisation du dispositif de sécurité, sensibilisation du personnel…)*

- **Mesures préventives :** *vérifier que des actions sont entreprises en cas de fraude détectée (à posteriori) : recouvrement, procédure pénale ; la diffusion et l'utilisation de mode.*
- **Mesures détectives :** *comprenant les mesures classiques de contrôle interne (états d'alerte, analyse de données a posteriori) et aussi les indices qui peuvent être des signaux faibles.*

[1] *Catégories issues de l'arbre de la fraude, partie 1.2, p. 14*

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

(Quels peuvent être les travaux et les mesures à mettre en œuvre au niveau opérationnel ?)

2- Actions au niveau du contrôle permanent (2ème niveau) :

(Quels peuvent être les travaux et les mesures à mettre en œuvre au niveau du contrôle permanent ?)

3- Actions au niveau de l'audit (3ème niveau) :

(Quels peuvent être les travaux de l'audit, en vue de s'assurer sinon de l'absence de fraude, du moins de l'existence d'un contrôle interne robuste diminuant le risque de fraude ?)

4- Actions par d'autres intervenants (A préciser) :

(selon le niveau de compétences et d'expertise requis)

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :

Signature :

© IFACI

© IFACI

ANNEXES

© IFACI

Annexe 1 : Grille de diagnostic préalable : Etat des lieux du dispositif anti-fraude

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Etat des lieux du dispositif anti-fraude : Que doit-on analyser en amont de toute action ?

Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
		Contributive	Souhaitable	Indispensable	
1 **Une capacité d'anticipation et des responsabilités clairement définies au niveau de l'organisation ?**					**Les rôles et responsabilités sont définis de manière appropriée par rapport à chaque organisation.** **L'organisation est proactive.** **Elle n'est pas uniquement en réaction par rapport à des cas avérés de fraude.**
	Un recensement des acteurs internes à mobiliser et une explication de leurs rôles respectifs dans le cadre du dispositif de lutte contre la fraude	X			Par exemple : métier, direction financière, direction juridique, resources humaines, système d'information, communication, etc.
	Une définition claire et partagée des rôles et des responsabilités des fonctions de contrôle interne par rapport à lutte contre la fraude	X			Selon les organisations, il peut s'agir de l'audit interne, de la direction de contrôle interne/contrôle permanent, de la conformité, de la direction des risques, de la sécurité financière, d'un service de lutte contre la fraude, etc.
	Des rôles pré-définis en matière de sensibilisation et de formation des collaborateurs	X			Un cadre général de réflexion qui intègre la formation de tous les acteurs.
	Une culture de décisions explicites et formalisées		X		La fraude n'est plus un sujet tabou.
	L'identification préalable des intervenants externes		X		Par exemple : les tutelles, les régulateurs, les CAC, l'équipe d'investigation externe, les assureurs, les autorités de police ou de justice.
	Un engagement officiel et visible de la direction générale concernant la lutte contre la fraude			X	Référence de documents ou minutes d'événements significatifs.
	Une structure hiérarchique organisée et connue de tous			X	Les gestionnaires sur le terrain savent à qui s'adresser et comment gérer les soupçons ou les cas avérés de fraude.

© IFACI

ANNEXE

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
2	**Des organes de gouvernance impliqués et informés ?**					**Le risque de fraude est suivi par les instances de direction et de gouvernance.**
		Le recours à une cellule de crise pour traiter des cas rencontrés est validé par les organes dirigeants.	X			Des scénarii de gestion de crise existent.
		Un comité spécialisé du conseil d'administration surveille le dispositif anti-fraude.	X			L'organe de gouvernance s'est saisi du risque de fraude et demande des informations sur ce sujet.
		Un membre du comité exécutif anime un comité éthique.	X			L'organisation a mené une réflexion sur l'éthique et s'est doté de moyens spécifiques.
		La gestion du risque de fraude est à l'ordre du jour des réunions du comité d'audit.		X		L'organe de gouvernance s'est saisi du risque de fraude et demande des informations sur ce sujet.
		La direction générale sponsorise la politique de lutte contre le rique de fraude.			X	Le directeur général ou l'un des membres du comité de direction a un mandat spécifique pour gérer le risque de fraude.
		Les opérationnels s'engagent à faire remonter tous les cas de fraude à leur hiérarchie.			X	Un élément important de la politique de gestion du risque de fraude dans le respect de la réglementation sur les données personnelles.

© IFACI

© IFACI

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
3	**Une politique anti-fraude formalisée est mise en œuvre ?**					**La gestion du risque de fraude va bien au-delà de l'incantatoire.**
		La politique fait l'objet d'une veille et d'une mise à jour.	X			Cette mise à jour concerne notamment les lois et réglementations relatives à la fraude en vigueur dans les pays où l'organisation opère.
		La détection comprend un volet d'analyse proactive de données susceptibles de révéler des fraudes.	X			Particulièrement lorsque de nombreuses transactions automatisées sont réalisées.
		Une procédure de gestion des risques de médiatisation est formalisée.	X			Prédéfinition d'une interface médias, questions/ réponses type préparation de la mobilisation de la cellule de crise, etc.
		Un protocole de traitement et d'investigation guide la mobilisation au cas par cas.	X			Définition des rôles et reponsabilités, de la cellule de crise et des acteurs (investigation, encadrement légal/ RH, etc.)
		La politique est cohérente avec les pratiques du secteur d'activité ou du metier exercé.		X		De nombreuses opportunités de comparaison existent pour chaque secteur d'activité.
		La politique anti-fraude est diffusée de façon traçable aux acteurs concernés.		X		Il s'agit des collaborateurs, des mandataires et éventuellement des clients ou des founisseurs.
		Les mandats des dirigeants aux différents échelons hiérarchiques font référence explicitement à leurs obligations en matière de lutte anti fraude.		X		
		Les rôles respectifs des fonctions centrales (métier, risques, audit, etc.) et des équipes locales en matière de lutte contre la fraude sont explicites.		X		
		La prévention anti-fraude comprend un volet sensibilisation/ formation/ communication destiné à l'ensemble du personnel.		X		Les médias et les messages sur la prévention peuvent éventuellement être segmentés selon la population visée (responsabilité, secteurs sensibles, etc.).

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
3	**Une politique anti-fraude formalisée est mise en œuvre ?** *(suite)*	Un reporting actualisé du traitement des cas en cours permet d'assurer un suivi, de construire une base de connaissance et d'alimenter des actions de prévention ou de détection.		X		Une cellule centrale est opératoire sur l'analyse des fraudes.
		Une politique anti-fraude est formalisée.			X	La gestion du risque de fraude peut comprendre notamment les définitions et conséquences, les principes et engagements de l'organisation, les rôles et responsabilités, les sanctions.
		La politique anti-fraude s'appuie sur une charte d'éthique ou un code de déontologie.			X	Le respect de la réputation des personnes et du droit sous-tend toutes les démarches entreprises, à chacune des étapes.
		Les principes de la politique et les procédures sont clairement accessibles à tous.			X	Cette diffusion s'appuie sur une communication et des formations internes appropriées.
		Un programme de lutte contre la fraude articulé, évolutif et planifié, est validé annuellement.			X	Ce programme doit être piloté avec la publication d'indicateurs clé d'avancement et d'efficacité, de rapports annuels présentés en Conseil d'administration et Comité d'audit.
		Les fraudes découvertes font l'objet d'une procédure de remontée/ escalade/ reporting formalisée aux instances de contrôle interne ?			X	Le respect de la réputation des personnes et du droit sous-tend toutes les démarches de l'organisation à chacune des étapes.

© IFACI

© IFACI

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
4	**Une cartographie spécifique du risque de fraude ?**					**Le repérage des risques de fraude est matérialisé par une démarche analytique anticipatoire.**
		Evaluation de la probabilité et de l'impact des risques recensés éventuellement pondérée par des risques "pays" ou "métier".	X			Etablissement de cartographies plus détaillées par secteurs géographiques ou domaines en cohérence avec la perception des risques.
		La cartographie est capitalisée sur des critères pertinents.	X			
		Une analyse actualisée avec les constats d'audits internes et externes.		X		
		La cartographie doit être accompagnée d'explications permettant au management de comprendre les enjeux.		X		Les explications peuvent contenir des exemples de fraude ou des indicateurs (exemple taux de démarque).
		Existence d'une typologie des fraudes potentielles liées aux secteurs d'activité de l'organisation.		X		Cette typologie doit être alimentée par la remontée des informations du management.
		Il existe une politique d'assurance (risque de fraude) cohérente avec les autres modalités de traitement.		X		Contre la politique d'assurance, les autres modalités de gestion du risque retenues dans la cartographie peuvent correspondre à des actions d'évitement, d'acceptation, de réduction et d'autres formes de partage du risque.
		Une approche intégrant tous les niveaux de l'organisation et conforme à la vision du top management.			X	La démarche d'analyse des risques est dotée des appuis et des moyens adaptés aux enjeux.
		Le management doit être sensibilisé préalablement aux spécificités des risques de fraude pour participer plus efficacement à leur mise en place.			X	Le management doit être convaincu que la fraude est un danger réel et doit connaître les cas classiques pouvant intervenir dans son domaine.
		Les cartes des risques sont liés à des plans d'actions qui doivent être suivis d'effets.			X	

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
5	**Des ressources proportionnées aux enjeux ?**					**Chaque organisation recense des acteurs internes ou externes à mobiliser selon ses niveaux de risques.**
		Des outils informatiques appropriés sont mobilisés pour détecter des situations à risque de fraude.	X			Pour gérer la question du seuil de matérialité, il convient de prendre en compte de multiples paramètres (montant, contexte, domaine, type de fraude, personnalité du fraudeur, etc.). Il est toujours difficile de définir un seuil de matérialité dans l'absolu : - un taux de « démarque inconnue » de X% dans un entrepôt ou un magasin sera dans un certain contexte « acceptable » (se traduisant par un préjudice de X€), - alors qu'une fraude avérée, portée à la connaissance du personnel et réalisée par un collaborateur « connu » d'un montant pourtant moindre aura un effet d'image important et ne sera donc pas toléré.
		Bases d'incidents formalisées, sécurisées, exploitées.	X			
		Des procédures spécifiques à certains métiers ou zone d'implantation sont adoptées.		X		
		Des contrôles automatisés sont effectifs pour prévenir l'occurrence d'un risque de fraude.		X		
		Les compétences "métier" sont mobilisées lors de la conception de la politique anti-fraude et pour sa mise en œuvre.		X		
		Les conditions de mobilisation de ressources externes sont clairement définies.		X		En tant que de besoin, recherche de compétences spécifiques (juristes, Certificated Fraud Examiner, etc.).
		La procédure de conservation des preuves est fomalisée et sécurisée.		X		

© IFACI

© IFACI

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
5	**Des ressources proportionnées aux enjeux ?** *(suite)*	Des procédures décrites et mises en œuvre pour chaque étape clé du dispositif.			X	Prévention, détection, traitement, correction.
		Les collaborateurs dédiés à la lutte contre la fraude sont compétents. En particulier, sur les volets détection et traitement.			X	Recrutements spécialisés ou sous-traitance.
6	**Un dispositif qui peut s'appuyer sur un système de contrôle interne déjà opérationnel ?**					**La lutte contre la fraude est difficilement opérationnelle sans culture du contrôle interne.**
		Statistiques sur les fraudes ou les indicateurs de fraude.	X			
		Les éléments du dispositif de contrôle interne sont examinés sous l'angle de leur contribution à la prévention de la fraude/ la détection.		X		
		Un dispositif de contrôle interne conforme aux référentiels est déployé.			X	L'existence d'un référentiel de contrôle interne s'appuie notamment sur : - un cadre éthique (code de conduite, règles d'éthique, normes déontologiques, etc.) effectif et appliqué par tous. - la politique de l'entreprise (définitions des responsabilités, des règles de délégations, des fiches de fonction...). - la structure organisationnelle qui doit refléter la politique de l'entreprise.
		Des outils de contrôle interne adaptés au contexte.			X	
		Mise en œuvre des contrôles internes et exploitation de leurs résultats.			X	

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
7	**Un audit interne efficient et coordonné avec les autres acteurs du dispositif ?**					**L'audit interne est un des vecteurs potentiel de sensibilisation à la fraude.**
		L'évaluation de l'efficacité du dispositif anti-fraude est réalisée régulièrement.	X			
		Le programme de travail des missions d'audit comprend l'évaluation des actions de prévention et de correction lorsque l'enjeu ressortant de la cartographie des risques le justifie.		X		
		La planification de l'audit interne tient compte de la cartographie du risque de fraude.		X		
		Les responsabilités de l'audit interne en matière de lutte contre la fraude sont définies dans la charte d'audit interne.			X	Respect des normes de l'IIA
		Le plan d'audit est fondé sur une approche par les risques qui comprend le risque de fraude.			X	
		Le responsable de l'audit interne rend régulièrement compte du risque de fraude et des contrôles correspondants à la direction générale et au comité d'audit.			X	
		Le programme de formation des auditeurs internes intègre le risque de fraude.			X	

© IFACI

© IFACI

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
8	**Un traitement des cas de fraude efficace ?**					**Le traitement des cas de fraude influe fortement sur l'efficacité du dispositif.**
		Existence d'une cellule de crise prête à gérer le dossier avec des responsabilités et des modalités de fonctionnement pré-établies.		X		La composition de la cellule de crise doit être anticipée. La cellule de crise doit planifier les mesures à prendre pour limiter le risque en fonction de la situation.
		Modalités claires et normées de remontée des informations permettant de mener l'investigation et d'évaluer les risques.		X		Existence de documents type et de canaux pour faire parvenir les informations rapidement et en toute confidentialité.
		Le management doit être alerté et formé sur les risques de fraude pour s'insérer plus facilement dans la démarche d'investigation et mieux comprendre les demandes dans le cadre des investigations.		X		Formation aux risques de fraude liés aux domaines d'activité.
		Le management doit être sensibilisé aux risques liés aux investigations à la fois sur les aspects sociaux et les aspects juridiques.		X		Formation aux risques de fraude liés aux domaines d'activité.
		Des procédures écrites doivent être mises en place et diffusées pour garantir la confidentialité, l'exhaustivité et l'efficacité des actions prévues.		X		Ne pas oublier les acteurs extérieurs (CNIL, assurances, police) et leurs modalités d'interaction avec les collaborateurs (exemple : manipulation des factures d'enquêteurs par la compabilité).
		Les retours d'expérience sont partagés.		X		Sensibilisation du management sur le mécanisme des fraudes traitées.
		Assurer la couverture juridique de la procédure pour éviter tout vice de forme.		X		Le service juridique doit être intégré dans la cellule de crise.
		Les dossiers de fraude doivent être clôturés, même si un doute persiste. Il faut accepter le fait de ne pouvoir conclure.		X		En cas de non-lieu, le dossier doit être clotûré de façon à ce qu'il n'y ait pas de doute sur les personnes impliquées.

Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
		Contributive	Souhaitable	Indispensable	
8 **Un traitement des cas de fraude efficace ?** *(suite)*	L'appel aux compétences internes et externes nécessaires pour les investigations doit être anticipé (responsabilités, disponibilités, règles de confidentialités).			X	Internes : Juridiques, Ressources Humaines, Informatiques, etc. Externes : Cabinet d'investigation ou de conseil juridique, enquêteurs, etc.
	Assurer un suivi des actions en lien avec les ressources humaines pour éviter les litiges.			X	La DRH doit participer à la cellule de crise.
	Des sanctions en ligne avec l'engagement de la direction générale.			X	Valeur d'exemplarité et d'appui à la politique.
	Des sanctions connues.			X	

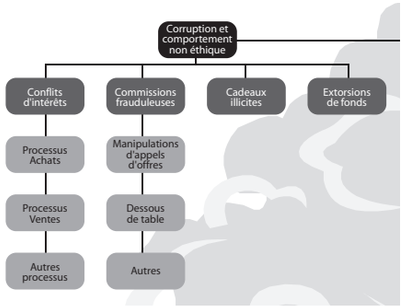
© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Annexe 2 : Illustration de l'arborescence des types de fraude

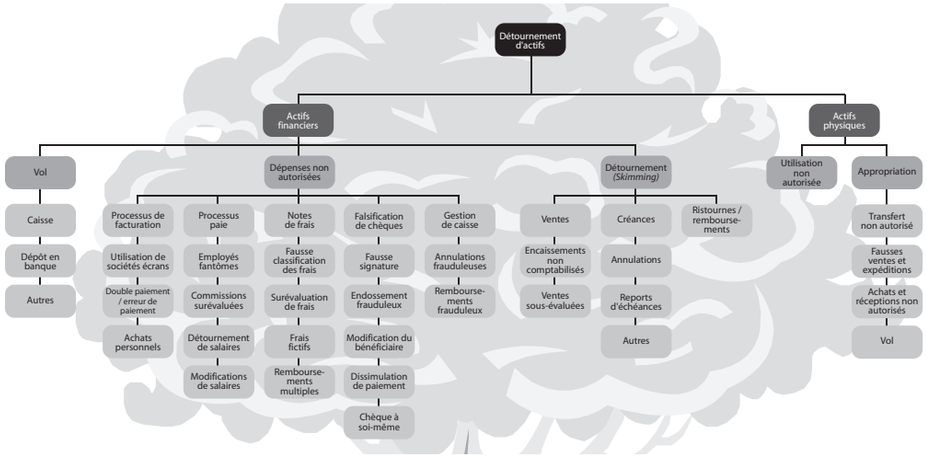
ANNEXE

© IFACI



Type	Sous-type	Exemple	Description
Corruption	Corruption et comportement non éthique / Commissions frauduleuses / Dessous de table	**Surfacturation**	Une organisation d'affichage retenue a proposé une offre spéciale. Après analyse précise des conditions de vente proposées par rapport à l'offre standard, l'offre spéciale proposée avait un coût supérieur de prés de 10 %.
		Surfacturation, favoritisme	Surfacturation de prestations / achats. Favoritisme vis-à-vis d'un fournisseur. Surfacturation de moyens commerciaux (remises et autres moyens).

© IFACI



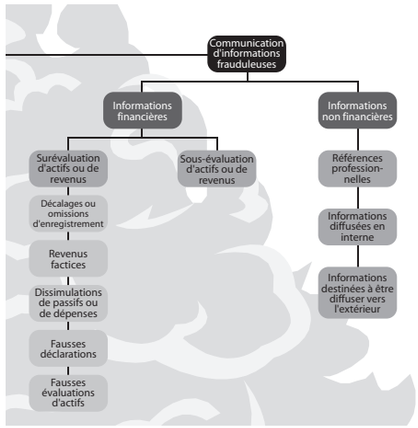
Type	Sous-type	Exemple	Description
Détournements d'actifs	Actifs financiers / Vol / Autres	**Falsification de prix**	Un responsable des ventes a utilisé le système de promotion dégressif de ventes des produits frais dont le prix est diminué en fonction du nombre de jours restant. En falsifiant la date de réservation, pour lui ou d'autres, il a pu finalement bénéficier de remises allant jusqu'à 80% dès les premiers jours de la promotion.
	Actifs financiers / Dépenses non autorisées / Note de frais	**Présentation de faux justificatifs**	Un employé a présenté dans ses notes de frais des tickets de parking non justifiés qu'il récupérait dans les machines du parking.
	Actifs financiers	**Encaissements différés**	L'employé, en charge des comptes clients et de l'encaissement, utilisait les encaissements à des fins personnelles et effectuait les paiements attendus par des emprunts sur les nouveaux encaissements. Il a également utilisé des chèques pour payer sur les autres comptes et récupérer les espèces versées. Pour ne pas éveiller les soupçons et élargir son temps d'emprunt, il reculait de plusieurs mois les dates d'échéances des factures dans le système. **Cet exemple montre à quel point les cas réels de fraude mixent différents éléments de la typologie proposée.**
	Actifs physiques / Appropriation	**Vols de produits impliquant un préparateur de colis**	Le préparateur mettait des produits supplémentaires sur les commandes des clients. Le chauffeur récupérait ensuite ces produits et les mettait en lieu sûr pendant sa tournée ou les revendait à des clients.
		Vols de produits impliquant un préparateur de colis	Le préparateur mettait des produits dans les poubelles présentes dans l'entrepôt, puis allait vider les poubelles dans les bennes à l'extérieur et mettait les produits dans son véhicule garé.

© IFACI

Type	Sous-type	Exemple	Description
Détournements d'actifs *(suite)*	Actifs financiers / vol / Dépôts en banque	**Utilisation des comptes clients créditeurs**	L'employé, en charge des comptes clients et de l'encaissement, utilisait d'anciens comptes clients créditeurs non clôturés pour créer des faux encaissements et il gardait les espèces.
	Actifs financiers / vol	**Détournement des fonds remis par les clients de l'organisation**	Cf. fiche 3 : Détournement de fonds pas un collaborateur, p. 115.
	Actifs financiers / Dépenses non autorisées / Processus de facturation	**Facturation frauduleuse de prestations / travaux à l'organisation**	Cf. fiches 7 et 8 : Prestations factices facturées à l'organisation, p. 128 et p. 131. Prestations réelles, détournées au profit de tiers.
		Détournements de moyens de paiement	Vol de chéquiers/ Lettres chèques, etc. Usurpation des habilitations de paiement informatisés (ordonnancement/ paiement, etc.). Fraude à la carte bancaire (et/ou fraude impliquant d'autres moyens de paiement tels que Paypal ou Fianet). Modification de RIB, de chèques. Cf. fiche 2 : Utilisation frauduleuse de moyens de paiement, p. 112.
	Actifs financiers / Dépenses non autorisées	**Usage de faux / Falsification**	Cf. Fiche 9 : Fausse pièces justificatives/dossiers de crédit, p. 134. Cf. fiche 10 : Falsification pièces justificatives d'un dossier entrée en relation, p. 138.
	Actifs physiques / Appropriation / Utilisation non autorisée	**Sortie frauduleuse en cours de transfert ou de transport**	Sortie frauduleuse en zone intermédiaire de stockage. Détournement de biens destinés à la destruction. Sortie frauduleuse en cours de transfert vers le client. Echange frauduleux de composants. Cf. fiche 1 : Echange frauduleux de composants informatiques, p. 109.
		Utilisation frauduleuse des moyens de l'organisation à des fins personnelles	Utilisation frauduleuse de budgets commerciaux, locaux de l'organisation, ou tous moyens (Informatique, de déplacement, etc.) mis à disposition par l'organisation. Cf. fiche 6 : Utilisation frauduleuse des moyens de l'organisation à des fins personnelles, p. 125.
			Cf. fiche 5 : E-commerce, p. 122. Cf. fiche 4 : détournements physique de matériel, p. 119

ANNEXE

© IFACI



Type	Sous-type	Exemple	Description
Manipulation d'informations	Informations non-financières / Informations diffusées en interne Ou Détournement d'actifs /Actifs financiers / Processus / Dépenses non autorisées / Processus paie	**Falsification de données intégrées dans le calcul des primes**	Les primes étant basées sur l'activité telle que suivie dans l'ERP, l'employé profitait des failles du système (possibilité de rajouter une personne, employé intérimaire non enregistré, absence de recoupement entre le système de suivi et le suivi des jours de présence) pour améliorer fictivement ses performances.
	Informations non financières / Informations destinées à être diffuser à l'extérieur	**Fraude fournisseurs**	Un fournisseur, facturé au poids, livrait le nombre exact de colis mais en réduisant le poids unitaire ce qui revenait à surfacturer le produit.

ANNEXE

© IFACI

Annexe 3 : Exemple de politique anti-fraude

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Politique de lutte contre la fraude

La présente politique définit la fraude et le dispositif de lutte contre la fraude. Elle présente les rôles et responsabilités des principaux acteurs vis-à-vis de la fraude.
Par ailleurs, les droits et devoirs de tout salarié de XXX sont définis dans le règlement intérieur de XXX, le code de bonne conduite ou la charte éthique à défaut.

1. Préambule

La société XXX prendra en compte toutes les remontées d'informations concernant des suspicions de fraude, vol et irrégularités et mènera des enquêtes approfondies.
La société établit et applique des procédures claires pour s'assurer que les enquêtes sont justes et respectent les personnes suspectées de fraude.
La société engagera des actions disciplinaires ou juridiques face à toute tentative ou tout acte de fraude avérée. Les fraudeurs doivent être conscients des conséquences négatives que peuvent avoir leurs actions sur leur avenir professionnel au sein de la société.
De plus, la politique de la société implique que tous les membres du personnel connaissent la procédure à suivre s'ils découvrent ou ont des raisons fondées de suspecter une fraude ou d'autres irrégularités au sein de XXX.

2. Qu'est-ce que la fraude ?

On peut définir la fraude comme « *tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services ou de s'assurer un avantage personnel ou commercial*[1] ».

La fraude peut se traduire par les actes suivants :

- Détournement d'actifs (utilisation de matériels de l'entreprise à des fins personnels, vol de produits ou d'espèces, remboursement frauduleux de frais de déplacements, etc.).

[1] *Définition de la fraude issue du glossaire, Cadre de Référence International des pratiques Professionnelles de l'audit interne, IIA/IFACI, janvier 2009.*

ANNEXE

© IFACI

- Montages frauduleux (enregistrement d'employés fictif, création d'un fournisseur fictif et de factures fictives, falsification de chèques, etc.).
- Manipulations des états financiers (écritures comptables fictives ou omission d'enregistrement comptable).
- Ententes avec un concurrent, avec un fournisseur (corruption passive), avec un client (corruption active).
- Conflits d'intérêts.
- Malveillance et sabotage.
- Fraude informatique.
- Abus de biens sociaux.
- Escroquerie.
- Etc.

Cette liste n'est pas exhaustive et vise à montrer la diversité des actes frauduleux.

3. Qui est concerné ?

La lutte contre la fraude est de la responsabilité de chacun au sein de XXX.

3.1- Responsabilité du management

La direction générale de XXX est responsable au sein de l'organisation de la prévention et de la détection des fraudes, des irrégularités et des erreurs. La direction générale pilote le dispositif de lutte contre la fraude. Elle délègue au management opérationnel le pilotage continu et le contrôle de ce dispositif.

3.2- Responsabilité de chaque salarié

Les salariés sont tenus de se conformer à la règlementation en vigueur en matière de lutte contre la fraude. Ils appliquent également les instructions de la direction générale dans ce domaine.

3.3- Responsabilité du traitement

La direction générale de XXX a désigné M. YYY comme responsable du traitement de la fraude.

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

4. Que dois-je faire si je suspecte ou découvre une fraude ou une irrégularité ?

4.1- Découverte et notification

Toute découverte ou suspicion de fraude impliquant un membre du personnel de XXX ou une personne extérieure à XXX devra être immédiatement signalée au responsable du traitement de la fraude qui évalue la gravité de la situation et en informe le Directeur financier, le Directeur des ressources humaines et le Directeur général, si nécessaire.
La remontée des informations se fera dans un délai de … heures. Une fiche de remontée de soupçon est à votre disposition. Vous pouvez également disposer d'autres modalités de notification telles que le dispositif d'alerte professionnelle.
Les données remontées par ces différents canaux seront gérées de manière confidentielle.

4.2- Investigation

Le responsable du traitement est chargé de mener les enquêtes sur les suspicions de fraude ou irrégularités.
Si l'incident doit entraîner une action disciplinaire, la direction des ressources humaines sera impliquée.
La recherche de preuves est essentielle pour vérifier les éléments qui ont amené à une suspicion de fraude. L'audit interne et la direction juridique devront valider l'approche à suivre et le niveau de détail nécessaire.

4.3- Importance du suivi de la procédure

Il est essentiel que la procédure soit suivie pour permettre une enquête juste et obtenir toutes les explications. Les personnes suspectées doivent être traitées avec équité, sans préjugé et aucune conclusion ne pourra être tirée sans examen approfondi des preuves.
Le défaut de procédure peut mettre en péril ou annuler tout recours légal ou mesure disciplinaire que la société souhaite prendre.

4.4- Confidentialité concernant l'incident

La fraude, avérée ou suspectée, ne doit pas faire l'objet de discussion et la confidentialité doit être maintenue. L'identité du fraudeur potentiel doit rester confidentielle.

© IFACI

4.5- Dénonciation calomnieuse

Toutes les remontées d'informations seront traitées avec la même rigueur et les mêmes conditions de sécurité. Néanmoins, toute dénonciation calomnieuse fera l'objet de sanction disciplinaire.

4.6- Suivi

Tous les cas de fraude seront suivis, tant que la décision de clôturer ces cas ne seront pas prises. La direction générale est régulièrement informée des procédures. Tous les cas de fraude avérés seront transmis au comité d'audit.

4.7- Récupération du préjudice

La récupération du préjudice subi (argent, stock) fera l'objet d'une action en collaboration avec la justice dans la mesure où la personne sera dans la possibilité de réparer le préjudice. Toute transaction, dans le but de récupérer le préjudice subi, sera établie sous l'autorité de la direction des ressources humaines.

© IFACI

Annexe 4 : Exemple de typologie de risques

© IFACI

Processus	Type de fraude	Exemple de risque de fraude	Exemple de contrôle anti-fraude
Achat	Communication d'informations financières frauduleuses	Sous-estimation des charges/ provisions …	- Suivi des évolutions prévisionnel/ réalisé ; n/n-1. - Analyse des écarts par le *disclosure* committee. - Politique de gestion du hors-bilan. - Etc.
	Détournements d'actifs	Achats fictifs …	- Procédures de contrôle interne relatives au décaissement d'espèces. - Contrôles intégrés dans l'application de gestion des ventes. - Etc.
	Corruption	Pots de vin et dessous de table	- Instructions sur la gestion des fournisseurs uniques, la sélection des fournisseurs. - Revue juridique et gestion des contrats. - Rapports détaillés de la part des sous-traitants. - Etc.
		Dissémination d'informations sensibles	- Code de bonne conduite. - Etc.
RH	Communication d'informations financières frauduleuses	Sous-estimation des charges/ provisions (exemple sur les congés payés)	- Suivi des évolutions prévisionnel/ réalisé ; n/n-1. - Contrôle hiérarchique. - Etc.
	Détournements d'actifs	Gestion de la paie (exemple, employés fictifs)	- Gestion des accès à l'application informatique liée à la paie. - Etc.
		Gestion des commissions et bonus	- Instructions sur la gestion des rémunérations et les modalités d'attribution/ validation. - Etc.
Stocks	Communication d'informations financières frauduleuses	Surévaluation des stocks	- Suivi de la valorisation des stocks et des dépréciations. - Contrôle automatique dans les ERP (écarts par rapports à des valeurs standards). - Etc.
	Détournements d'actifs	Larcins	- Sécurité des accès physiques. - Rapprochement inventaire physique/ registre comptable. - Etc.
	Corruption	Dissémination d'informations sensibles (exemple sur la sécurité)	- Classification des informations sensibles et gestion de leur accès. - Etc.

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Processus	Type de fraude	Exemple de risque de fraude	Exemple de contrôle anti-fraude
Gestion des CAPEX	Communication d'informations financières frauduleuses	Sous-évaluation des charges	- Contrôle interne au niveau de la gestion des dépréciations, gestion des amortissements, R § D, etc. et contrôle de la classification. - Etc.
	Détournements d'actifs	Vols	- Contrôle aléatoire des employés à la sortie du site. - Etc.
	Corruption	Pots de vin et dessous de table (exemple, en phase de désinvestissement)	- Procédure de contrôle interne pour l'approbation des Capex. - Etc.
Taxes	Communication d'informations financières frauduleuses	Sous-évaluation/ surévaluation des actifs	
	Détournements d'actifs	Evasion fiscale	- Compétences fiscales dans les entités majeures. - Implication du département « fiscalité » pour les contrats à l'export ou des refacturations internes au Groupe. - Etc.
	Corruption	Pots de vins	- Comparaison des taxes par entités. - Etc.
Trésorerie	Communication d'informations financières frauduleuses	Sous-évaluation des dettes	- Procédures de gestion des processus de trésorerie (dettes, ristournes, etc.). - Experts en trésorerie au niveau central. - Etc.
	Détournements d'actifs	Vol d'espèces	- Coffre-fort. - Procédure d'approbation et de gestion des sorties d'espèces. - Etc.
	Corruption	Blanchiment	- Revue des contrats par la conformité/ le département juridique. - Etc.
Autres	Détournements d'actifs	Fusions acquisitions	- Formalisation de la stratégie d'investissement. - Etc.
	Corruption	Cyber-criminalité	- Tests d'intrusion. - Etc.

ANNEXE

© IFACI

Annexe 5 : Fiches

Détournement d'actifs	1. Echange frauduleux de composants informatiques 2. Utilisation frauduleuse de moyens de paiement 3. Détournement de fonds par un collaborateur 4. Détournement physique de matériel 5. E-commerce
Corruption et comportement non éthique	6. Utilisation frauduleuse des moyens de l'organisation à des fins personnelles 7. Prestations factices facturées à l'organisation 8. Prestations factices facturées à l'organisation
Communication d'informations frauduleuses	9. Fausse pièces justificatives/dossiers de crédit 10. Falsification pièces justificatives dossier entrée en relation

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Echange frauduleux de composants informatiques

Fiche n° : *1*

Classification :
- ☑ Fraude interne
- ❑ Fraude externe

Type de fraude : *Détournement physique de matériel*

Canal de détection :
Contrôle opérationnel :
- *Désordre physique récurrent au sein du local informatique.*
- *Absence de zone dédiée et sécurisée de stockage des matériels neufs d'une part et ancien d'autre part.*

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ☑ Dirigeant /Manager
- ☑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :……...

Identification des parties prenantes et/ou de l'activité concernées : *DSI*

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Lors de la campagne d'échange des postes de travail informatiques au sein d'une entité, des collaborateurs remplacent frauduleusement les nouveaux composants (extraits des nouveaux postes) par des vieux composants (extraits des anciens postes). Les vieux postes ainsi rénovés, sont ensuite revendus par les individus concernés, au lieu d'être détruits.
En revanche, l'entreprise intègre sans le savoir dans son parc des composants obsolètes.

ANNEXE

© IFACI

Evénement générateur - Causes - Défaillances :

- *Absence de procédure de désinvestissement des matériels.*
- *Absence de procédure de suivi des investissements.*
- *Mauvaise séparation des tâches entre utilisateurs (opérationnels de la fonction informatique) et gestionnaires des investissements.*

Facteurs aggravants de risques détectés : ☑ oui ❑ non

Si oui, nature du facteur aggravant : *Inventaire irrégulier ou mal maîtrisé.*

Catégorie de fraude :

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournement d'actifs financiers
- ☑ Détournement d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ☑ Moyen
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :

- ☑ Pertes financières,
- ☑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

© IFACI

Evaluation financière, si pertinente :

Perte brute : ……

% récupéré : ……

Perte nette : ……

Charges d'investigation : ……

Mesures correctrices envisagées :

- **Mesures préventives :** *Vérification du processus de mise au rebut et signature des bons de mise au rebut ; identification et mise à l'écart des anciens matériels, traitement par une équipe indépendante des opérationnels ; Séparation des tâches entre utilisateurs des investissements et gestion des investissements ; Zone dédiée et sécurisée de stockage des matériels neufs d'une part et anciens d'autre part.*
- **Mesures détectives :** *Procédure robuste de désinvestissement : Contrôle Physique des entrepôts et magasins de toute sorte ; Enquête sur toute zone de stockage laissée en désordre ; Visite des locaux informatiques.*

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

- *Formalisation de la mise au rebut*
- *Séparation des tâches*

2- Actions au niveau du contrôle permanent (2ème niveau) :

- *Enquêtes sur les zones de stockage*
- *Vérification de l'application des procédures*

3- Actions au niveau de l'audit (3ème niveau) :

- *Analyse de la procédure de désinvestissement et de son contrôle*

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :

Signature :

© IFACI

Utilisation frauduleuse de moyens de paiement

Fiche n° : *2*

Classification :
- ☑ Fraude interne
- ❑ Fraude externe

Type de fraude : *Utilisation frauduleuse de moyens de paiement*

Canal de détection :
- *La réclamation du client qui s'est rendu compte de la fraude.*
- *Le chargé de compte de la banque (récupération des fonds par la banque, qui se fait directement sur le compte du commerçant et à son insu).*
- *La suspension temporaire de la transaction en cas de suspicion*

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ☑ Dirigeant / Manager
- ☑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :……...

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Utilisation frauduleuse de moyens de paiements (Carte bleue ou hybride tels que Paypal, Fia-Net ...) : Vol d'un moyen de paiement type Carte Bleue ou usurpation d'identité pour un paiement hybride tel que paypal afin d'effectuer des achats à distance.

ANNEXE

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Evénement générateur - Causes - Défaillances :
- *Un manque probant de contrôle lors de la validation humaine du paiement.*
- *Un logiciel de validation automatique des modes de paiements qui n'est pas régulièrement mis à jour.*
- *Peu d'actions entreprises en cas de fraude détectée, ce qui augmente les risques.*

Facteurs aggravants de risques détectés :
- ☑ oui
- ❑ non

Si oui, nature du facteur aggravant : *L'enregistrement des données bancaires au sein même de l'organisation lors des transactions peut être un facteur aggravant, car en cas de piratage ce sont des milliers de personnes qui pourraient être touchées par la fraude.*

Catégorie de fraude :
- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ☑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ☑ Détournement d'actifs financiers
- ❑ Détournement d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**
- ❑ Mineur
- ❑ Moyen
- ❑ Important
- ☑ Majeur
- ❑ Critique

Nature de l'impact :
- ☑ Pertes financières,
- ❑ Pertes de productivité
- ☑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ☑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

ANNEXE

© IFACI

Evaluation financière, si pertinente :
Perte brute : .....
% récupéré : .....
Perte nette : .....
Charges d'investigation : .....

Mesures correctrices envisagées :

- **Mesures préventives :** *Diminuer au maximum les validations de commande humaine très gourmandes en termes de main d'œuvre et avec un risque élevé d'erreur du fait de la subjectivité de chacun ; veiller une mise à jour permanente du logiciel de validation automatique des commandes.*
- **Mesures détectives :** *Suivi des transactions exceptionnelles.*

Détermination du « Qui fait quoi » en fonction du point précédent :
➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

2- Actions au niveau du contrôle permanent (2ème niveau) :

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :
Signature :

ANNEXE

© IFACI

Utilisation frauduleuse de moyens de paiement

Fiche n° : *3*

Classification :
☑ Fraude interne
❑ Fraude externe

Type de fraude : *Détournements de fonds par un collaborateur*

Canal de détection :
Appel téléphonique au service audit du responsable de l'agence bancaire du collaborateur en raison de mouvements de fonds importants sur son compte, tous en provenance de la même société.

Date de détection : *juin année n*

Origine de la fraude :
❑ Prospect ou Client
❑ Tiers non identifié
❑ Dirigeant / Manager
☑ Salarié
❑ Fournisseur ou Prestataire
❑ Autre (préciser) :……....

Identification des parties prenantes et/ou de l'activité concernées :
Responsable du Service Commissions courtiers

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Un collaborateur a détourné des commissions affectées à des courtiers dont le statut était codifié « en déshérence ». Lors d'un changement d'attribution d'un portefeuille ou de disparition d'un courtier, les commissions calculées sur les primes encaissées sont toujours affectées au code du courtier ayant réalisé l'affaire. Mais ces commissions ne peuvent être libérées qu'après attribution du portefeuille à un nouveau courtier.
Date des faits : *avril année n*

ANNEXE

© IFACI

Evénement générateur - Causes - Défaillances :

- *Le collaborateur bénéficiait d'un double rattachement dans l'organigramme de la société.*
- *L'un de ses rattachements lui permettait de connaître tous les courtiers en déshérence et donc le montant des commissions bloquées.*
- *Son second rattachement, au département Gestion, lui permettait de disposer d'habilitations informatiques grâce auxquelles il a modifié 1°) les coordonnées bancaires existant dans les bases en y reportant son propre numéro de compte, 2°) le code de blocage des commissions. Le blocage étant supprimé, les commissions étaient alors virées automatiquement sur le nouveau compte bancaire introduit dans les bases.*

La faille était donc due à ce double rattachement, ainsi qu'à une non séparation de tâches incompatibles entre elles.

Facteurs aggravants de risques détectés :
☑ oui
❑ non

Si oui, nature du facteur aggravant : *Insuffisance de contrôle interne. Problème d'organisation et de tâches incompatibles entre elles, confiées à un même collaborateur.*

Catégorie de fraude :

❑ Conflits d'intérêts
❑ Commissions frauduleuses
❑ Cadeaux illicites
❑ Extorsions de fonds
❑ Informations financières frauduleuses
❑ Informations non financières frauduleuses
☑ Détournement d'actifs financiers
❑ Détournement d'actifs physiques
❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

❑ Mineur
☑ Moyen car fraude rapidement arrêtée
❑ Important
❑ Majeur
❑ Critique

© IFACI

Nature de l'impact :

☑ Pertes financières,
❑ Pertes de productivité
❑ Pertes commerciales (exemple nombre de clients affectés)
❑ Préjudice humain
❑ Préjudice réglementaire ou juridique
❑ Détérioration de l'image de marque
❑ Autre (préciser) : ……

Evaluation financière, si pertinente :

Perte brute : *200 000 €*

% récupéré : *190 000 €, le collaborateur n'ayant pas eu le temps de dépenser les sommes détournées avant que l'alerte soit remontée au service audit de la compagnie.*

Perte nette : *10 000€ (avant procédure judiciaire).*

Charges d'investigation : .....

Mesures correctrices envisagées :

- **Mesures préventives :** *Séparation des tâches. Nouvelle organisation des services Gestion et Commissions courtiers.*
- **Mesures détectives :** *comprenant les mesures classiques de contrôle interne (états d'alerte, analyse de données a posteriori).*

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

- *Licenciement du collaborateur.*
- *Mise en œuvre des mesures préventives.*

2- Actions au niveau du contrôle permanent (2ème niveau) :

- *Analyse des données.*

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

© IFACI

ANNEXE

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

- *Suivi, avec les directions juridique et les ressources humaines, de l'action judiciaire destinée à récupérer les fonds.*
- *Suivi de la réorganisation des services et de la bonne séparation des tâches.*
- *Contrôle de la mise en place d'instructions concernant la modification des RIB des courtiers dans les bases (problème des habilitations informatiques).*

Nom du rédacteur :

Date :
Signature :

© IFACI

Détournement physique de matériel

Fiche n° : *4*

Classification :
- ❑ Fraude interne
- ☑ Fraude externe

Type de fraude : *Sortie frauduleuse de matériel informatique situé dans les bureaux des collaborateurs du siège*

Canal de détection :
Constatation de la disparition d'ordinateurs portables par les collaborateurs à leur arrivée le matin.

Date de détection : *janvier année N*

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant / Manager
- ❑ Salarié
- ❑ Fournisseur ou Prestataire
- ☑ Autre (préciser) : *Salarié d'un prestataire*

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Ces vols se sont étalés sur plusieurs jours. Des travaux étant effectués dans l'immeuble, la première enquête, diligentée dès la constatation des premiers vols, a porté sur les entreprises intervenant sur le site, les ouvriers entrant et sortant par une entrée non surveillée en permanence par un gardien. De plus, ils pouvaient circuler sans contrainte dans l'ensemble de l'immeuble. Une surveillance permanente de cette issue a été immédiatement mise en place.
Comme les vols ont continué, une seconde enquête a été effectuée et a permis de comprendre le mécanisme du vol : le prestataire, chargé d'alimenter les distributeurs de boissons répartis dans les étages, profitait des horaires matinaux de ses interventions pour couper les antivols et dissimuler les ordinateurs dans les cartons sous les produits non mis dans les appareils.

© IFACI

Evénement générateur - Causes - Défaillances :
Contrôle physique des accès.

Facteurs aggravants de risques détectés : ☑ oui ❑ non

Si oui, nature du facteur aggravant : *Absence de procédure et d'instructions remises aux gardiens concernant le contrôle des cartons ou emballages sortant de l'établissement.*

Catégorie de fraude :

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournement d'actifs financiers
- ☑ Détournement d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ☑ Moyen
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :

- ☑ Pertes financières,
- ☑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

ANNEXE

© IFACI

Evaluation financière, si pertinente :

Perte brute : *Valeur des portables volés, mais difficulté d'évaluer la perte des données et de productivité en découlant.*

% récupéré : *Valeur des portables remboursés par le prestataire + somme forfaitaire transactionnelle pour le préjudice relatif à la perte de données et de productivité.*

Perte nette : *Perte des données et de productivité difficilement quantifiables malgré le règlement d'une indemnité transactionnelle.*

Charges d'investigation : .....

Mesures correctrices envisagées :

- **Mesures préventives :** *Surveillance des accès avec contrôle des emballages sortants, fermeture à clé des bureaux individuels, vidéosurveillance.*
- **Mesures détectives :** *Analyse de données a posteriori et aussi d'indices tels que la persistance des vols de différents types (matériel de l'entreprise ou affaires personnelles de collaborateurs.*

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

- *Mise en place de contrôle physique des emballages sortants.*

2- Actions au niveau du contrôle permanent (2ème niveau) :

- *Vérification de l'existence de procédures de contrôle des accès aux immeubles.*

3- Actions au niveau de l'audit (3ème niveau) :

- *Tester l'existence des procédures et l'efficacité des contrôles en tentant de faire sortir du matériel par des tiers « assermentés ».*

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Suivi de la mise en cause du prestataire, suivi de l'action judiciaire et/ou de la transaction financière destinée à compenser le préjudice subi. Suivi de la résiliation du contrat avec le prestataire. Suivi de la mise en place des procédures de surveillance des allers et venues dans les immeubles, en particulier de contrôle des sorties d'emballages.

Nom du rédacteur :

Date :

Signature :

ANNEXE

© IFACI

E-commerce

Fiche n° : *5*

Classification :
- ❑ Fraude interne
- ☑ Fraude externe

Type de fraude : *Détournement physique de matériel*

Canal de détection :
La récurrence des pertes lors du transport sur un une zone donnée, un numéro de plomb différent de celui inscrit sur le bon de livraison.

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant / Manager
- ❑ Salarié
- ☑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Sortie frauduleuse en cours de transfert vers le site : Il s'agit en fait d'un détournement du fait du transporteur. La marchandise est effectivement sortie de la centrale d'achat avec un numéro de tracking colis mais celui-ci n'arrive jamais en magasin.

Evénement générateur - Causes - Défaillances :
Un mauvais filmage des palettes laissant entrevoir le contenu de la marchandise, ainsi qu'un mauvais cerclage.

Facteurs aggravants de risques détectés :
- ❑ oui
- ☑ non

Si oui, nature du facteur aggravant :

ANNEXE

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Catégorie de fraude :
- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournements d'actifs financiers
- ☑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**
- ❑ Mineur
- ☑ Moyen
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :
- ☑ Pertes financières,
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

Evaluation financière, si pertinente :
Perte brute : *1 000 € à 10 000 € en fonction de la quantité*
% récupéré : .....
Perte nette : .....
Charges d'investigation : .....

ANNEXE

© IFACI

Mesures correctrices envisagées :

- Mesures préventives : *S'assurer que les palettes sont bien filmées avec un film noir, la présence du cerclage avec un bon de garantie avant l'expédition, que le numéro de plomb a bien été inscrit sur le bon de livraison ; Au niveau du transport, s'assurer de la présence de vigile lors du retrait ou dépôt de marchandise. Un moyen de prévention serait de conclure un contrat de transport qui inclurait des pénalités financières en cas d'avarie, de la perte totale ou partielle pourrait se produire pendant la période de transport. Mais ce moyen de prévention a ses limites dans la mesure où la pénalité financière n'est qu'une indemnité et ne couvre que rarement la globalité des biens perdus.*
- Mesures détectives : *A la réception, un contrôle de l'état général de la marchandise avant signature du bon de livraison, une vérification de la cohérence des numéros de plombs ; Une procédure de signalement immédiat de tout colis ou palette manquante ; Une vérification mensuelle des écarts de livraison dans les points de ventes et, en cas de non signalement, demander des comptes au responsable du point de vente.*

Détermination du « Qui fait quoi » en fonction du point précédent :
➔ 3 axes : détection – prévention – contrôle
1- Actions au niveau opérationnel (1er niveau) :

2- Actions au niveau du contrôle permanent (2ème niveau) :

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :
Signature :

© IFACI

Utilisation frauduleuse des moyens de l'entreprise à des fins personnelles

Fiche n° : *6*

Classification :
☑ Fraude interne
❑ Fraude externe

Type de fraude : *Utilisation frauduleuse de moyens de l'entreprise*

Canal de détection :
Refus de mobilité de carrière vers des postes qui éloignent d'un « terroir » très contrôlé.
Proximité excessive de certains subordonnés, sous couvert de développer un esprit d'équipe gagnant.

Date de détection :

Origine de la fraude :
❑ Prospect ou Client
❑ Tiers non identifié
☑ Dirigeant / Manager
❑ Salarié
❑ Fournisseur ou Prestataire
❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Un responsable d'exploitation jouissant d'une excellente réputation pour avoir géré avec succès la construction et la mise en opération de nouvelles unités de production performantes et créé un fort esprit d'équipe dans ses unités, s'est appuyé sur son réseau de collaborateurs proches et inféodés à son autorité pour faire payer par la société des dépenses correspondant à un hobby personnel (modèles réduits d'avion pour lesquels il s'est fait payer par l'entreprise de l'outillage et un atelier mobile). Il a par ailleurs autorisé des voyages et séminaires sans réelle justification professionnelle pour sa « garde rapprochée ».

© IFACI

Evénement générateur - Causes - Défaillances :

Compte tenu de ses succès professionnels, tangibles et encensés, ce dirigeant a sans doute développé un sentiment de grande autonomie par rapport au reste de l'organisation et à ses règles du jeu. Les montants détournés pour alimenter son hobby étaient faibles (25kEuros +) par rapport aux montants qu'il gérait pour les projets professionnels (chiffrés en dizaines de millions d'Euros). Sa hiérarchie a perdu les repères de contrôle basique, ou n'a pas osé challenger quelqu'un de si forte réputation (signaux faibles ignorés deux ans avant la mise à jour de la fraude).

Facteurs aggravants de risques détectés : ☑ oui ❑ non

Si oui, nature du facteur aggravant : *Attitude de confiance érigée en principe intouchable (pour créer et entretenir un esprit d'équipe gagnante), qui peut masquer un fonctionnement autocrate et manipulateur, particulièrement lorsqu'un manageur semble « charismatique ».*

Catégorie de fraude :

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ☑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ❑ Moyen
- ☑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :

- ❑ Pertes financières,
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ☑ Préjudice humain
- ☑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Evaluation financière, si pertinente :

Perte brute : .....

% récupéré : .....

Perte nette : .....

Charges d'investigation : .....

Mesures correctrices envisagées :

- **Mesures préventives :** *Créer une ligne éthique qui permet une remontée anonyme de dysfonctionnements managériaux ; vérifier régulièrement (par sondage) les comptes de dépenses des dirigeants ; assurer la séparation des tâches pour que le responsable local ne puisse pas approuver seul les demandes d'achats qu'il aura autorisées ; vérifier que les achats techniques correspondent aux nécessités des opérations (registre des fournisseurs et numérotation des pièces de rechange).*
- **Mesures détectives :** *Rigueur de gestion des remboursements de frais. Le supérieur hiérarchique généralement éloigné dans le cas de managers seniors doit s'assurer d'une vérification effective des dépenses de ses subordonnés ; Sensibilité aux signaux faibles et aux discordances d'effets de « clique ».*

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

2- Actions au niveau du contrôle permanent (2ème niveau) :

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :

Signature :

ANNEXE

© IFACI

Prestations factices facturées à l'entreprise

Fiche n° : *7*

Classification :
- ☑ Fraude interne
- ❑ Fraude externe

Type de fraude : *Prestations factices à des fins personnelles*

Canal de détection :
Compte fournisseurs divers volumineux et non pointé.

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant / Manager
- ☑ Salarié
- ☑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Un Cadre d'entreprise réussit à facturer à l'entreprise des prestations dont il bénéficie en réalité à titre personnel : travaux de terrassement, génie civil, entretien paysager de son domicile, etc.

Evénement générateur - Causes - Défaillances :
- *Absence de processus achat*
- *Absence de procédure de réception administrative robuste (pas de vérification par le client de la réalité de la prestation)*
- *Processus d'ordonnancement faible (réconciliation commande - réception de la prestation - facture)*

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Facteurs aggravants de risques détectés :
- ☑ oui
- ❑ non

Si oui, nature du facteur aggravant : *Rotation insuffisante sur les postes*

Catégorie de fraude :
- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ☑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournements d'actifs financiers
- ☑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**
- ❑ Mineur
- ❑ Moyen
- ☑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :
- ❑ Pertes financières,
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ☑ Préjudice humain
- ☑ Préjudice réglementaire ou juridique
- ☑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

Evaluation financière, si pertinente :
Perte brute : *1 000 € à 10 000 € en fonction de la quantité*
% récupéré : .....
Perte nette : .....
Charges d'investigation : .....

© IFACI

Mesures correctrices envisagées :

- Mesures préventives : *Processus Achat robuste ; Processus de réception robuste ; Processus d'ordonnancement des factures ; Double signature au-delà d'un certain seuil, tant pour le paiement que pour la réception.*
- Mesures détectives : *Revue des comptes fournisseurs divers ; revue des prestations dites intellectuelles, œuvres caritatives, conseil, ensemble des prestations immatérielles.*

Détermination du « Qui fait quoi » en fonction du point précédent :
➔ 3 axes : détection – prévention – contrôle
1- Actions au niveau opérationnel (1er niveau) :

2- Actions au niveau du contrôle permanent (2ème niveau) :

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :
Signature :

© IFACI

Prestations factices facturées à l'entreprise

Fiche n° : *8*

Classification : ☑ Fraude interne
❑ Fraude externe

Type de fraude : *Détournement de fonds de l'entreprise par factures*

Canal de détection :
Compte fournisseurs divers volumineux et non pointé.

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ☑ Dirigeant / Manager
- ❑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Un Directeur Financier réussit à détourner des fonds au profit d'escrocs, sous mention de prestations de conseils fictives. (Diverses variantes).

Evénement générateur - Causes - Défaillances :
Absence de processus achat, de procédure de réception administrative robuste (pas de vérification par le client de la réalité de la prestation).
Le Directeur Financier avait pouvoir de signature illimité, sans double signature : Processus d'ordonnance

Facteurs aggravants de risques détectés : ☑ oui
❑ non

Si oui, nature du facteur aggravant : *Rotation insuffisante sur les postes*

© IFACI

Catégorie de fraude :

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ☑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ☑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ❑ Moyen
- ❑ Important
- ☑ Majeur
- ❑ Critique

Nature de l'impact :

- ☑ Pertes financières
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

Evaluation financière, si pertinente :

Perte brute : .....

% récupéré : .....

Perte nette : .....

Charges d'investigation : .....

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Mesures correctrices envisagées :

- **Mesures préventives :** *Processus Achat robuste ; Processus de réception robuste ; Processus d'ordonnancement des factures ; Double signature au-delà d'un certain seuil, tant pour le paiement que pour la réception.*
- **Mesures détectives :** *Revue des comptes fournisseurs divers, des prestations dites intellectuelles, œuvres caritatives, conseil, ensemble des prestations immatérielles.*

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

2- Actions au niveau du contrôle permanent (2ème niveau) :

3- Actions au niveau de l'audit (3ème niveau) :

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :

Signature :

ANNEXE

© IFACI

Fausses pièces justificatives – Dossier de crédit

Fiche n° : *9*

Classification :
- ☑ Fraude interne
- ☑ Fraude externe

Type de fraude : *Mise en place de dossiers de crédits avec des fausses pièces justificatives et complicité client – commercial et collaborateurs back office*

Canal de détection :
Contrôle permanent et tiers.

Date de détection :

Origine de la fraude :
- ☑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant / Manager
- ☑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :
Réseau commercial et Back office chargé de l'enregistrement des dossiers de crédits.

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Complicité entre le client, le commercial réseau et un collaborateur du back office crédit dans l'objectif de mettre en place des dossiers de crédits qui, au vu du profil du client et des revenus réels de ce dernier, ne pouvaient être légitimement accordés.

Evénement générateur - Causes - Défaillances :
Défaillance des processus de contrôle opérationnel (séparation de tâches, autorisation, contrôle manager).

© IFACI

Facteurs aggravants de risques détectés :
- ☑ oui
- ❑ non

Si oui, nature du facteur aggravant : *Réorganisation du back office, changement de manager, augmentation sensible de l'activité, turn-over important, insuffisance des ressources allouées.*

Catégorie de fraude :
- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ☑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ☑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**
- ❑ Mineur
- ❑ Moyen
- ☑ Important *(30 dossiers concernés pour un montant moyen de 10 000 €)*
- ❑ Majeur
- ❑ Critique

Nature de l'impact :
- ☑ Pertes financières
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

© IFACI

Evaluation financière, si pertinente :
Perte brute : *300 000 €*
% récupéré : *80% (remboursement direct de certains dossiers et mise en place d'un échéancier de remboursement pour d'autres dossiers)*
Perte nette : *50 000 € (avant procédure judiciaire)*
Charges d'investigation : .....

Mesures correctrices envisagées :

- **Mesures préventives :** *Actualisation du dispositif de contrôle a priori ; sensibilisation des collaborateurs et du management, renforcement de l'effectif du back office.*
- **Mesures détectives :** *Actualisation du dispositif de contrôle a posteriori.*

Détermination du « Qui fait quoi » en fonction du point précédent :
➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

- *Revue du dispositif de contrôle opérationnel dans son ensemble*
- *Actualisation des procédures, mise en place d'une nouvelle organisation*
- *Revue du processus de séparation des tâches*
- *Revue du montant de délégations de pouvoir*
- *Renforcement du contrôle « manager » (mise en place d'un contrôle exhaustif ou aléatoire des dossiers en fonction des montants engagés)*

2- Actions au niveau du contrôle permanent (2ème niveau) :

- *Renforcement des contrôles sur place et sur pièces, échantillonnage.*
- *Contrôle de l'actualisation et de la stricte application des procédures par l'ensemble des intervenants*
- *Actualisation du plan de contrôle annuel, suivi de la mise en œuvre de la nouvelle organisation*

3- Actions au niveau de l'audit (3ème niveau) :

- *Vérification du dispositif de contrôle interne et de la mise en œuvre des mesures correctives*
- *Suivi des actions mises en œuvre par le contrôle opérationnel et le contrôle permanent*
- *Actions de sensibilisation auprès du réseau commercial*

4- Actions par d'autres intervenants (A préciser) :

© IFACI

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :
Modification des autorisations internes et des processus d'enregistrement des dossiers ; Procédure de licenciement des collaborateurs concernés ; Actions en justice pour récupération des sommes indûment versées ; traitement et suivi des différents dossiers déclarés (actions clients, actions et sanctions collaborateur interne et collaborateur réseau commercial…).

Nom du rédacteur :

Date :
Signature :

© IFACI

Falsification de pièces justificatives d'un dossier entrée en relation

Fiche n° : *10*

Classification :
- ❑ Fraude interne
- ☑ Fraude externe

Type de fraude : *Falsification pièces justificatives dossier entrée en relation*

Canal de détection :
Contrôle opérationnel.

Date de détection :

Origine de la fraude :
- ☑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant / Manager
- ❑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :

Identification des parties prenantes et/ou de l'activité concernées :
Réseau commercial et Back office chargé de l'enregistrement des dossiers d'entrée en relation et ouverture de compte.

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
Un nouveau client a manifestement falsifié les documents transmis pour son ouverture de compte à laquelle était associée une demande d'ouverture d'un crédit à la consommation.
Les bulletins de salaire transmis ont été modifiés (modification de la profession, faux employeur, modification du revenu net).

Evénement générateur - Causes - Défaillances :
Défaut de contrôle du dossier à l'origine par commercial réseau.
Non respect des procédures de vigilance et de vérification prescrites.

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Facteurs aggravants de risques détectés :
- ❑ oui
- ☑ non

Si oui, nature du facteur aggravant :

Catégorie de fraude :
- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ☑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : ……

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**
- ❑ Mineur
- ☑ Moyen *car fraude rapidement arrêtée.*
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :
- ☑ Pertes financières
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : ……

Evaluation financière, si pertinente :
Perte brute : *10 000 €*
% récupéré : *100% (dossier d'ouverture de compte refusé)*
Perte nette : *aucune*
Charges d'investigation : .....

© IFACI

Mesures correctrices envisagées :

- Mesures préventives : *Sensibilisation du réseau commercial sur les vérifications à réaliser sur l'authenticité des pièces justificatives transmises par le client.*
- Mesures détectives :

Détermination du « Qui fait quoi » en fonction du point précédent :

➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :

- *Externe (réseau) : renforcement des contrôles préventifs*
- *Interne (back office) : renforcement des contrôles sur la cohérence des pièces justificatives et en particulier les bulletins de salaire transmis*

2- Actions au niveau du contrôle permanent (2ème niveau) :

- *Renforcement de l'échantillonnage de contrôle sur les dossiers clients*
- *Vérification du respect des procédures par le réseau commercial*
- *Actions de sensibilisation du réseau commercial et des différents responsables du contrôle interne*

3- Actions au niveau de l'audit (3ème niveau) :

- *Vérification de la qualité du dispositif de contrôle interne*

4- Actions par d'autres intervenants (A préciser) :

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :
Signature :

© IFACI

BIBLIOGRAPHIE

© IFACI

© IFACI

BIBLIOGRAPHIE

Dispositions réglementaires et de place

Recommandation AMF n°2010-07 du 3 novembre 2010 : Guide relatif à la prévention des manquements d'initiés imputables aux dirigeants des sociétés cotées / AMF

Ordonnance n°2008-1278 du 8 décembre 2008 transposant la directive 2006/43/CE du 17 mai 2006 et relative aux commissaires aux comptes
Publiée au Journal officiel n°0286 du 9 décembre 2008 (p. 18720) – [Transposition de la 8e directive]

Loi n°2008-561- du 17 juin 2008 portant réforme de la prescription en matière civile
Publiée au Journal officiel n° 0141 du 18 juin 2008 (p. 9856)

Document d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés / Commission Nationale Informatique et Libertés - 2005.

Ordonnance du 2 novembre 1945 relative au statut des huissiers (Version consolidée au 01 février 2009).
Publiée au JORF du 3 novembre 1945 (p. 7163)

Code pénal
- Art. 311-1
- Art. 313-1
- Art. 314-1
- Art. 323-1 à 323-7
- Art. 441-1

Foreign Corrupt Practices Act (FCPA) / Etats-Unis – 1979

© IFACI

Référentiels professionnels et enquêtes

1- Audit interne et contrôle interne

Cadre de référence international des pratiques professionnelles de l'audit interne [CRIPP] / IIA, IFACI trad. – 2009 *(mise à jour prévue en 2011)*

Internal auditing and fraud: IPPF – practice guide / IIA. - 2009.

Prise de position IFA/IFACI sur le rôle de l'audit interne dans le gouvernement d'entreprise. – IFA ; IFACI. – 2009.

L'urbanisme du contrôle interne : comment en améliorer l'efficacité ? Quelle place pour l'audit interne ? Prise de position / IFACI. – 2008.

Managing the business risk of fraud: a practical guide / IIA, AICPA, ACFE. – 2008

Internal control and internal auditing, guidance for directors, managers and auditors / ECIIA. – 2000

Position paper on the internal auditor's role in the prevention of fraud / ECIIA. – 1999
Le Rôle de l'auditeur interne dans la prévention de la fraude : Prise de position de l'ECIIA, octobre 1999, (European Confederation of Institutes of Internal Auditing) / IFACI – 2000

Saywer's internal auditing: The practice of modern internal auditing, 5th ed. / Lawrence B. Sawyer, Mortimer A. Dittenhofer, James H. Scheiner. – 2003

Management override of internal controls: The Achilles' heel of fraud prevention / The audit committee and oversight of financial reporting. – 2005

2- Fraude

L'Audit de la fraude dans le secteur bancaire / Groupe Professionnel « Banque » – IFACI -- 2010

Report to the Nations on Occupational Fraud and Abuse / Association of Certified Fraud Examiners – 2010

Pour un bon dispositif de lutte contre le blanchiment des capitaux : Secteur bancaire / Groupe Professionnel "Banque" – IFACI -- 2004

European fraud Survey 2009 / Ernst & Young – 2009
Enquête 2009 sur la fraude en Europe (trad. de European Fraud Survey 2009) - Rapport France / Ernst & Young – 2009

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Enquête 2009 sur la fraude dans les entreprises en temps de crise (trad.. de PwC Global Economic Crime Survey 2009 – France) / PWC – 2009

Fraud red flags tool / Protiviti – 2000

SAS 99 Consideration of Fraud in a Financial Statement Audit, Statement of Accounting Practices / American Institute of Certified Public Accountants. – [2007]

Histoires ordinaires de fraudes / ACFE Chapitre Français – 2010

Tackling external fraud / HM Treasury ; National Audit Office – 2009

Fraud Prevention Checkup / ACFE - 2008

Fraud Prevention and Detection in an Automated World: global technology audit guide (GTAG®) 13, IPPF Practice Guide / IIA. - 2009.

3- Corruption / Ethique

Rapport Mondial sur la corruption 2009 : La corruption et le secteur privé / Transparency International. – 2009.

Driving ethical growth — new markets, new challenges: 11th Global Fraud Survey / Ernst & Young. – 2010

Knowledge Alert: Emerging Trends in Fraud Risks / IIA. – 2010

Commission de réflexion pour la prévention des conflits d'intérêts / Transparence International France – 2010

Global Fraud Report 2009-2010 / KROLL. – [2009]

© IFACI

Ouvrages

L'investigation informatisée des fraudes : recherche informatisée et Prévention / Noël PONS, Yoanna PONS. – 2010

La fraude en entreprise – Comment la prévenir, la détecter, la combattre / Mikael OUANICHE. – 2009

Power, Ambition, Glory: The Stunning Parallels Between Great Leaders of the Ancient World and Today... and the Lessons You Can Learn / Steve FORBES ; John PREVAS. – 2009

Executive Roadmap to Fraud Prevention and Internal Control / Martin T. BIEGELMAN, Joel T. BARTOW. – 2009

Cyber Fraud : Tactics, Techniques, and Procedures / James GRAHAM et al. – 2009

Selected Writings / Joseph T. WELLS. – 2009

Interviwing and Interrogation – Second Edition / Don RABON. – 2009

Computer Fraud Casebook – The Bytes that Bite. - Joseph T. WELLS (editor) – 2009

Arnaques : Le manuel anti-fraude / Noël PONS ; Valérie BERCHE – 2009

Corporate Resiliency – Managing the Growing Risk of Fraud and Corruption / Toby J.F. BISHOP ; Frank E. HYDOSKI. – 2009

Fraud Risk Assessment – Building a fraud audit program / Leonard W. VONA. – 2008

Fraude connection : en finir avec les arnaques sociales / Geoffroy FOUGERAY. – 2007

Encyclopedia of Fraud - Third Edition / Joseph T. WELLS. - 2007

Cols blancs et mains sales : Economie criminelle, mode d'emploi / Noël PONS. – 2006

The World's Largest Hedge Fund is a Fraud: Submission to the SEC / Harry MARKOPOLOS. – 2005

Internal Controls Guide / Wanda A. WALLACE. – 2005

Audit et fraude / Noël PONS. – 2004

© IFACI

LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Halte aux Fraudes : Prévenir et détecter les fraudes en entreprise / Olivier GALLET. – 2004

Auditing accounts payable for fraud / David G. BANKS. – 2001

Million-dollar frauds / Gary McKECHNIE ; Nancy HOWELL. – 1998

Fraud examination for managers and auditors / Jack C. ROBERTSON. – 1997

Face à la corruption / Michel BON. – 1993

How to detect fraud through auditing / Alan JACOBSON. – 1990

The Cuckoo's Egg: Tracking A Spy Through The Maze Of Computer Espionage / Clifford STOLL. – 1989

Deterring Fraud: The internal auditor's perspective / Steve ALBRECHT ; Marshall B. ROMNEY ; Keith R. HOWE. – 1984

Foozles and frauds / Harold F. RUSSELL. – 1977

"Affaires"

No One Would Listen: A True Financial Thriller / Harry MARKOPOLOS. – 2010

L'Affaire Madoff / Amir WEITMANN. – 2009

Extraordinary Circumstances: The Journey of a Corporate Whistleblower / Cynthia COOPER. – 2008

Stolen Without A Gun: Confessions from inside history's biggest accounting fraud - the collapse of MCI Worldcom / Walter PAVLO Jr. – 2007

Final Accounting: Ambition, Greed and the Fall of Arthur Andersen / Barbara Ley TOFFLER ; Jennifer REINGOLD. – 2003

Power failure: the inside story of the collapse of Enron / Mimi Swartz ; Sherron Watkins ; Doubleday – 2003

The Smartest Guys in the Room: The Amazing Rise and Scandalous Fall of Enron / Bethany McLEAN. – 2003

© IFACI

Réalisation : Ebzone Communication (www.ebzone.fr)
Impression : Compédit Beauregard S.A. - 61600 La Ferté-Macé
N° d'imprimeur : 4475