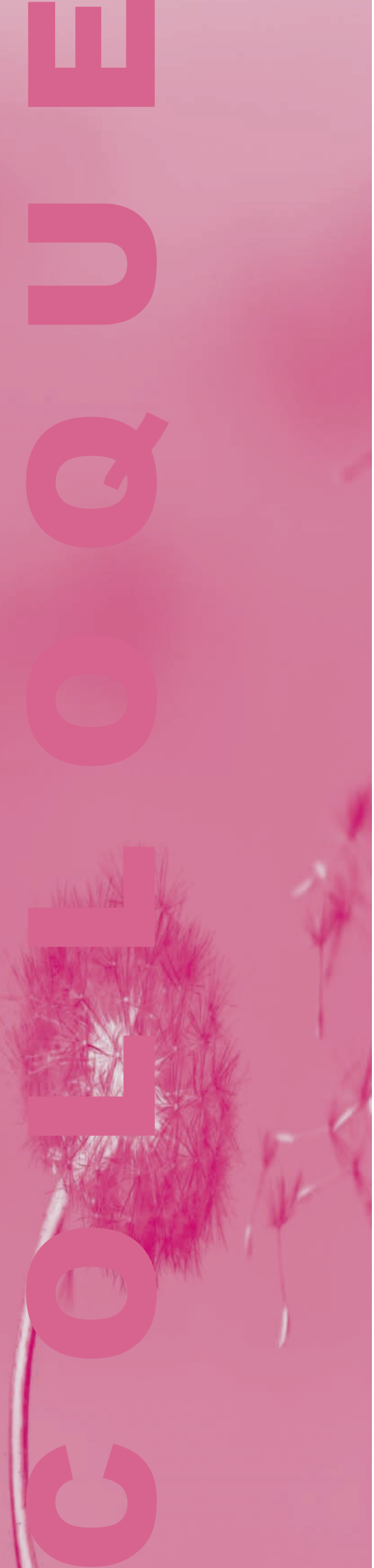
COLLOQUE



Institut de l'Audit Interne

ACTES DU COLLOQUE

La fraude : les dispositifs de prévention, de détection et de traitement

- jeudi 31 mai 2007 -

© IFACI - Paris - Avril 2008
ISBN : 978-2-915042-16-0

SOMMAIRE

Discours introductif 5

Panorama des différents mécanismes de fraude - les indicateurs 5

Les étapes-clés de la mise en œuvre des dispositifs de prévention, détection et traitement de la fraude et de la corruption 10

Liens entre les mécanismes de montage de fraude et les mécanismes de blanchiment 16

Comment intégrer des modules de prévention de la fraude dans la gestion de projets ? 18

Comment un auditeur peut-il identifier le risque de corruption privée dans l'entreprise ? 23

Témoignage : Les contrôles transversaux dans les administrations 25

Les problématiques de traitement des fraudes dans les filiales étrangères 28

L'entreprise, cible des fraudeurs : comment l'audit interne peut-il la protéger ? 33

Bibliographie 41

© IFACI

© IFACI

Discours introductif

Noël PONS, ***CIA, Conseiller, Service Central de Prévention de la Corruption***

Pourquoi encore un colloque sur les fraudes ? Parce que s'ouvre, devant nous, un nouveau champ d'investigation ; un champ d'investigation que certains connaissent depuis plus de trente ans, d'autres depuis moins longtemps. Mais qu'a-t-on comme base d'analyse ? Une complexité des ensembles économiques constante. Chaque société dispose maintenant de dix, vingt, trente ou cent filiales. Contrôler la fraude dans les filiales n'est pas chose aisée ; il y aura, cet après-midi, une intervention sur ce type de mission. Et les opérations de sous-traitance, délocalisation, re-sous-traitance, sous-traitance en cascade : autant d'occasions de « s'amuser » avec des factures.
La réduction des délais de traitement des données nécessite une obligation de travailler dans l'urgence, avec les conséquences qui en découlent.
La financiarisation de l'économie nous donne des vapeurs, si j'ose dire, puisque les éléments sont de plus en plus sophistiqués. Vous m'expliquerez comment vous allez comptabiliser et quels contrôles vous allez mettre en place dans votre entreprise, sur un certificat CO2 qui est délivré par une société non reconnue et de gré à gré.
Enfin, la criminalité fait son entrée dans la fausse facturation, et là, on change de niveau.
Pour toutes ces raisons ce colloque se justifie.
Nous allons commencer avec Olivier GALLET qui va nous dresser un panorama des différents mécanismes de fraude, et nous parler des indicateurs.

Panorama des différents mécanismes de fraude – les indicateurs

Olivier GALLET, ***Expert-comptable, OGL-Audit***

Bonjour. Mon expérience professionnelle est double puisque je suis commissaire aux comptes et que j'ai également exercé en tant que responsable d'audit interne. Je me suis intéressé à la fraude parce qu'ayant rencontré des cas dans mes deux activités, je me suis rendu compte que les méthodes utilisées n'étaient pas adaptées, ce qui m'a conduit à écrire un ouvrage intitulé « Halte aux fraudes » et à fonder un cabinet spécialisé, OGL-Audit, utilisant ces nouvelles méthodes.

Si l'on parle les fraudes internes, on peut distinguer deux catégories : la fraude des employés et la fraude financière. L'ACFE *(Association of Certified Fraud Examiners)*, qui a beaucoup travaillé sur ces sujets, appelle la fraude financière : *Management Fraud*. Je préfère l'appellation « fraude financière », qui est plus claire, le *Management*, pour nous, désignant l'encadrement responsable.
Les fraudes des employés sont normalement accomplies contre l'entreprise par les employés, dont le management, parfois même par des personnes de haut niveau. Le but du jeu, c'est de détourner des biens ou des valeurs. Ces détournements représentent près de 80 % des fraudes, parfois avec des schémas de corruption, de prise illégale d'intérêt, et des collusions avec un tiers extérieur.

© IFACI

Les fraudes financières, que j'ai connues en tant que commissaire aux comptes, ont pour objectif d'améliorer la situation financière de l'entreprise, en surévaluant les produits. Outre le bilan, le compte de résultats et les annexes, tous les états financiers sont concernés : les *reportings* trimestriels, les tableaux de bord de gestion, et autres états qui servent à payer des commissions ou des bonus. C'est ainsi que les fraudes financières en faveur de l'entreprise rejoignent souvent les fraudes des employés, car il y a toujours une ou plusieurs personnes intéressées dans le montage d'une fraude.

Aujourd'hui, nous allons surtout nous intéresser à la fraude des employés, c'est-à-dire celle qui est menée contre l'entreprise. Un schéma classique de fraude comporte des mécanismes récurrents se déroulant toujours en trois étapes.

La première étape consiste à faire sortir les valeurs de l'entreprise. Ce qui vous impose, à vous auditeurs, de vous demander où sont les valeurs de l'entreprise. Les valeurs de l'entreprise sont disséminées un peu partout, donc souvent on en oublie, ce qui fait l'affaire des fraudeurs. Il faut donc recenser toutes les valeurs. Je pense par exemple aux entreprises qui ne protègent pas leurs lettres-chèques en se disant que tant qu'elles ne sont pas imprimées, elles ne valent rien. De même pour les bordereaux de virement : un bordereau de virement vierge, avec une bonne procédure de virement, devient une valeur. De même encore pour des tickets, dans une agence de voyages : un bordereau de ticket vierge est une valeur.
Le but du fraudeur est donc de faire sortir des valeurs de l'entreprise, si possible discrètement. Mais très souvent, la discrétion ne paie pas, et en particulier pour les stocks ; il vaut mieux agir en pleine journée, au vu de ses collègues, et mettre simplement des marchandises dans un autre camion que celui qui était prévu : on fait ainsi tranquillement sortir les stocks de l'entreprise. Cette méthode est valable pour les valeurs physiques. Pour les valeurs monétaires, cela dépend du lieu où elles sont rangées : dans un tiroir-caisse, ou dans un compte en banque. Pour des sommes situés sur un compte en banque, il s'agit de provoquer une dépense fictive ou de détourner des moyens de paiement.

La deuxième étape consiste à dissimuler la disparition, pour ceux qui travaillent dans l'entreprise et veulent y rester. (Si le fraudeur est externe, le problème de dissimulation ne se pose pas, parce qu'il a pris ses dispositions pour ne pas être retrouvé ; je pense en particulier aux virements frauduleux sur des comptes étrangers). Le fraudeur pense souvent qu'il rendra l'argent plus tard ; c'est pendant cette période de latence qu'il lui faut dissimuler.

La troisième étape, que l'on découvre de temps en temps, et que je mentionne, bien que vous n'ayez, à mon avis, aucune possibilité d'action, **c'est la conversion**. La conversion consiste à transformer ce que l'on a volé en quelque chose d'utilisable. Si j'ai détourné un chèque qui est à l'ordre de l'entreprise, il va falloir que je le convertisse pour pouvoir l'encaisser sur un compte en banque, soit en modifiant l'ordre, soit en créant un compte bancaire à cet ordre-là. Si je vole des stocks, il va falloir que je les écoule sur un marché. Il y a eu beaucoup d'affaires concernant des ouvriers qui volaient des éléments sur des chaînes, reconstituaient des produits et les vendaient sur le marché situé juste à côté de l'entreprise, le samedi.
Dans la technique des schémas de fraude, on se met à la place du fraudeur et l'on se demande : « Qu'est-ce qui va l'empêcher de frauder ? » Ce qui l'empêche, ce sont ces trois éléments sur lesquels vous devez agir : l'empêcher de faire sortir les valeurs de l'entreprise, grâce au contrôle interne ; rechercher les indicateurs nés de la dissimulation de la disparition ; quant à la conversion, il est difficile d'agir dessus.

Les schémas de fraude, si on les étudie, permettent de les reconnaître, et donc les détecter. La lutte contre la fraude, en matière d'audit, n'est pas un élément que l'on traite à part, mais fait partie du cadre des problèmes généraux d'audit. Seulement, en examinant un processus, on va se focaliser sur certains éléments, parce que l'on va chercher des schémas de fraude. Pour chaque processus on identifie un schéma de fraude en rapport avec l'environnement. Chaque schéma comprend deux volets : un volet prévention et un volet détection. Le volet prévention concerne les contrôles qui empêchent le schéma de se réaliser : sont-ils suffisants, sont-ils efficaces ? Lorsque je réalise des audits, je constate souvent que des contrôles existent, mais que les personnes

 © IFACI

chargées de leur mise en œuvre n'ont pas conscience de l'importance de ces contrôles, qui deviennent, par le fait, inopérants. Le volet détection : si le schéma se réalise malgré les contrôles, c'est-à-dire si le fraudeur contourne ces contrôles, des symptômes vont apparaître, révélés par des indicateurs qui identifieront une fraude.

Examinons le processus achats. Il commence à la commande et se termine au paiement. A quelle étape le fraudeur doit-il se placer pour frauder le plus facilement possible ? Au paiement il a accès à l'argent tout de suite ; il détourne le paiement et il dissimule. A la commande, c'est faisable aussi, à condition de créer toute une série de faux (papier ou informatique) qui vont supporter la chaîne : faux bon de commande, faux bon de réception, fausse facture, etc., bref, de respecter le processus de l'entreprise. C'est donc plus simple d'agir à la fin ; c'est ce que font d'ailleurs la plupart des fraudeurs.

On distingue, dans le processus achats, des schémas de facturation et des schémas de corruption. Je vous parlerai des schémas de facturation. On les appelle ainsi parce qu'ils reposent sur le processus de facturation de l'entreprise. On en distingue trois.

Le premier, c'est le fournisseur fictif : le fraudeur va créer un faux fournisseur ou il va en réactiver un ancien qui existe déjà, ce qui lui permet de justifier une documentation fictive : le bon de commande, le bon de réception, la facture (ou informatique). Il met l'ensemble dans le circuit de paiement, qu'il connaît très bien, récupère ensuite le paiement tout à fait légitime qui est émis, et il va l'encaisser.
En tant qu'auditeur, vous devez vous demander quels problèmes le fraudeur doit résoudre pour réussir l'opération. D'abord créer le fournisseur fictif, par exemple une société fictive, une SARL, ce qui n'est pas très compliqué en France : il suffit d'attestations sur l'honneur, d'une copie de carte d'identité… A la tête de la SARL, il faut mettre un gérant, le fraudeur lui-même en général. Ensuite, il faut ouvrir un compte bancaire ; c'est peut-être un peu plus délicat, car il faut un K bis, etc., mais cela peut se faire. Enfin il faut créer toute la documentation fictive et l'insérer dans le circuit de paiement.
Les contrôles, s'ils sont en place et opérants, doivent empêcher le fraudeur de réaliser ces opérations, et, en tout cas, font apparaître un certain nombre d'indicateurs : par exemple, le paiement à des fournisseurs qui ne figurent pas dans le fichier des fournisseurs ; des paiements à des fournisseurs dont l'adresse correspond à celle d'employés ou qui est suspecte ; le paiement à des fournisseurs « réactivés » : c'est beaucoup plus simple que d'en créer un faux ; des paiements à des fournisseurs dont le montant dépasse largement le paiement moyen ; ou encore l'utilisation d'un fournisseur dont le RIB (ou l'adresse) sera modifié(e), etc.

Le deuxième schéma est le paiement indirect. Le principe est de faire payer une facture en double. On réutilise la documentation d'une facture réelle, et on la remet dans le circuit de paiement. Comment récupère-t-on le paiement en double ? Par exemple en l'interceptant, avant qu'il parte chez le fournisseur. C'est le cas, lorsqu'un collaborateur dit : « je vais porter directement le chèque au fournisseur. » C'est un signal d'alerte auquel le personnel doit être sensible : il n'est pas normal de prendre un chèque pour le remettre directement au fournisseur.
Il est possible aussi de faire envoyer le chèque et d'appeler ensuite le fournisseur en lui disant : « Il y a un problème, on vous a payé en double. Renvoyez-nous le chèque. », et le fraudeur donne son adresse du bureau. C'est pourquoi, une sage précaution consiste à faire enregistrer le courrier arrivé et particulièrement les valeurs comme les chèques.
Là aussi des indicateurs peuvent mettre la puce à l'oreille : une tendance à la hausse des paiements à un fournisseur ; les variations de charges par fournisseur ou par service ; une tendance à la hausse du coût d'achat des articles ; des comptes fournisseurs comprenant des doublons (numéros de factures, de bons de commande…). Les outils d'analyse informatique permettent de déceler les paiements en double : c'est un indicateur mais ce n'est pas forcément une fraude.

Le troisième schéma est la falsification de moyens de paiement, chèques ou virements.
Pour détourner des chèques, il faut avoir accès à ces chèques. Une règle de base de contrôle interne, est de

conserver les carnets de chèques en lieu sûr (coffre-fort), de les inventorier régulièrement, et d'en limiter l'accès à des personnes désignées.
Le fraudeur qui parvient à mettre la main sur un chéquier, imite une signature autorisée et réalise un paiement non justifié. La procédure est identique pour le virement : un faux virement, généralement en faveur d'une banque étrangère, est remis à la banque de l'entreprise. Ensuite, il va falloir dissimuler l'opération, cacher cette dépense injustifiée. Pour ce faire, il existe un certain nombre de comptes : les comptes de TVA déductible ; les comptes fournisseurs que personne ne surveille ; des comptes de charges ; des comptes intragroupes, parfois, quand j'ai un complice qui me fait la réciprocité ; même des comptes d'actif : j'ai vu des œuvres d'art que personne n'avait jamais remarquées, et qui cachaient des détournements.
Les indicateurs, sur ce type de schéma, seront des comptes fournisseurs non justifiés, d'où l'intérêt de faire des circularisations ; pas sur les gros montants mais sur les fournisseurs qui paraissent suspects. Et il faut analyser les comptes susceptibles de dissimuler le paiement.

Le processus vente comprend aussi différents schémas.

Le détournement de chèques clients. Le chèque arrive dans l'entreprise, et quelqu'un l'intercepte, au courrier par exemple si la procédure de ce service est mauvaise ou inexistante.
Pour dissimuler la disparition, un moyen existe qui s'appelle le *lapping*. Le but du jeu est de détourner un encaissement d'un client ; quand le deuxième encaissement du même client arrive, on rembourse le premier, et ainsi de suite. Les comptes clients n'étant jamais justifiés, les anomalies n'apparaîtront pas forcément.
Les relances constituent un bon contrôle interne, mais elles sont rarement utilisées. Elles permettent d'avertir le client qu'il se passe quelque chose dans son compte. A condition de les envoyer : j'ai déjà vu des paquets de relances au pied des bureaux, parce qu'on ne voulait pas les envoyer ; ou des relances avec des mauvaises adresses ; ou avec des anomalies de codification, etc. Autres exemples d'indicateurs : on peut comparer le délai client par client ; circulariser les comptes clients ; examiner les comptes de clients présentant des écritures d'ajustement ; analyser les réclamations des clients ; comparer les écritures d'encaissement avec les bordereaux de remise (il y aura des écarts en cas de *lapping*).

Les techniques de facturation en matière de vente, consistent à réaliser, par exemple, des ventes fictives pour obtenir un avantage, une commission, une prime sur objectif – c'est presque de la fraude financière – ou à réaliser des ventes réelles à titre personnel en utilisant sa position dans l'entreprise. On utilise les schémas de facturation de l'entreprise, on fait des ventes, et l'entreprise n'est pas au courant. Il y a souvent un risque quand les commerciaux vont directement sur place. Il y a vente de marchandise mais la vente n'apparaît pas dans l'entreprise, ou alors pas pour le même montant.
Même méthode sur la caisse et la trésorerie. On distingue deux schémas : ce qui se passe *off book*, c'est-à-dire que l'argent est prélevé dans la caisse, sans enregistrement ; ce qui se passe *on book*, c'est-à-dire que la vente est enregistrée et ensuite, un avoir, une remise, un remboursement sont enregistrés pour faire sortir l'argent. Les schémas *on book* sont réalisés par les caissiers, les schémas *off book*, par les gérants qui vont faire, comme par hasard, des opérations d'ajustement le soir, à la fermeture. Ces opérations peuvent être décelées par l'examen des états de caisse détaillés.

Les stocks et immobilisations : il s'agit essentiellement du vol de marchandises ou de produits, et du vol ou de l'utilisation personnelle d'immobilisations.
Le vol de marchandises peut être réalisé soit en faisant croire à une vente, soit sans support. Il sera décelé lors d'un inventaire. Deux possibilités : le fraudeur cherche à dissimuler ou pas. Si c'est un magasinier lambda, il ne cherche pas à dissimuler : il y aura un écart dans le stock, mais on ne remontera jamais jusqu'à lui. Si c'est le responsable du stock, il sait qu'on va lui taper sur les doigts il va donc chercher à dissimuler, ce qui veut dire passer des écritures dans l'inventaire permanent, des écritures non justifiées, pour ajuster. Ces écritures, vous devez pouvoir les retracer.
La méthode des schémas consiste à imaginer comment opère le fraudeur, quels contrôles peuvent l'empêcher d'opérer, et quels indicateurs permettent de détecter la fraude.

© IFACI

L'utilisation personnelle d'immobilisations est liée aux ressources humaines.

Le processus paye est aussi un support de fraude, puisqu'il permet de sortir de l'argent tous les mois.
La première méthode est de créer un salarié « fantôme ». En France c'est extrêmement difficile, en raison notamment des déclarations aux organismes sociaux. Mais n'oubliez pas qu'il peut y avoir des filiales, parfois, dans des pays étrangers qui n'ont pas du tout la même réglementation ; et dans ces filiales, il est possible de créer des salariés fantômes. C'est donc un risque qu'il faut que vous traitiez.
C'est le même principe que le fournisseur fictif : que demande-t-on pour créer un salarié ? Parfois, selon la répartition des pouvoirs, il suffit que le directeur de l'usine envoie un courrier au service paie, accompagné de certains documents, et le salarié fictif est créé. Après, il va falloir le faire vivre, lui régler des primes, des heures supplémentaires, etc. J'ai vu ce schéma-là au Canada, qui portait sur vingt salariés fictifs créés par une personne travaillant à la paie. La paie est une fonction sensible qu'il faut surveiller. L'indicateur, dans le domaine des salariés fantômes, peut être l'absence de mouvement sur les congés payés.
Une deuxième méthode est celle des commissions et des données variables. Il faut savoir comment sont calculées les commissions, à partir de quels documents, et qui contrôle ces documents.
Une troisième méthode est celle des remboursements de frais. Sur ces remboursements, il y a quatre indicateurs : des dépenses non justifiées, des relevés de frais « gonflés », des dépenses fictives, et des remboursements multiples. Une personne se fait rembourser, par exemple, le billet d'avion validé par tel service, et puis se fait rembourser la facture de l'agence de voyage, signée par un autre service. Une personne prend un billet de 1ère classe, l'annule, prend un billet de 2ème classe, et se fait rembourser le billet de 1ère. Ce sont des petits larcins, mais qui traduisent un mauvais état d'esprit dans l'entreprise ; c'est pour cela que vous devez lutter contre la fraude.

Vous allez me dire : « nous sommes des auditeurs internes, en quoi les schémas de fraude nous concernent-ils ? »
Effectivement, les normes disent que l'auditeur interne n'a pas la responsabilité d'enquêter sur les fraudes ; ce n'est pas son travail. En revanche, elles disent aussi que l'auditeur doit posséder des connaissances suffisantes pour identifier les indices d'une fraude. Pour ce faire, vous devrez travailler concrètement sur vos processus, avec les schémas, les indicateurs, les signaux d'alerte, et apprendre à réagir en présence d'anomalies. Attention toutefois à rester dans un rôle d'auditeur pour garder un esprit critique sur le système et ne pas être amené à trop intervenir dans les procédures. C'est pourquoi il est intéressant de travailler avec un expert extérieur sur ce sujet.

QUESTIONS

Noël PONS

J'aimerais poser une question assez simple : comment arrive-t-on, lorsqu'on est « normalement » formaté à inverser la vapeur pour entrer dans un cheminement de fraud examiner, de chasseur ?

Olivier GALLET

Il y a effectivement un problème psychologique. D'ailleurs, on le voit bien, quand une affaire de fraude survient dans une entreprise, souvent la direction est un peu perdue, et ne sait quoi faire. Généralement elle se tourne vers l'audit.
Aux Etats-Unis, dans les études de CPA (l'équivalent de l'expertise comptable en France), il y a obligatoirement des cours sur les fraudes, en particulier par les schémas. En France, ce sera le cas bientôt. J'ai été surpris, en relisant l'examen du CIA récemment, de voir un grand nombre de parties sur la fraude qui n'existaient pas il y a cinq ans. On demande maintenant aux auditeurs d'être vigilants, d'être capables de repérer des indicateurs et de savoir que c'est un risque comme un autre qu'ils doivent traiter.

Louis VAURS, *Délégué Général, IFACI*

Il est vrai que l'on constate un intérêt croissant sur les aspects de la fraude. Ce que vous dites concernant le CIA est tout à fait vrai, et on le voit d'une manière générale dans toute la documentation que l'on peut lire. Il y a une pression de plus en plus forte sur les auditeurs internes.
J'aimerais savoir si, vous-même, avez découvert des fraudes. Lorsqu'on lit les statistiques, on constate que la quasi-totalité des fraudes ont été trouvées par hasard ou bien dans le cadre d'un whistleblowing performant, dans le cadre de dénonciations diverses.
J'ai pratiqué ce métier pendant très longtemps. Chaque fois que j'ai eu affaire à des fraudes, c'est par l'intermédiaire de dénonciations, de lettres ou de coups de téléphone anonymes.
Avez-vous trouvé des fraudes directement ?

Olivier GALLET

Depuis que j'utilise cette méthode-là, oui. J'ai découvert quatre ou cinq fraudes sur les achats ou les chèques détournés. Mais il est vrai qu'il m'est arrivé d'auditer des cycles achats fournisseurs sans rien découvrir, et c'est le client qui a détecté la fraude.

Les étapes-clés de la mise en œuvre des dispositifs de prévention, détection et traitement de la fraude et de la corruption

Noël PONS

Nous allons parler maintenant des étapes clés de la mise en œuvre des dispositifs de prévention, détection et traitement de la fraude et de la corruption.
Ces activités seront présentées par Antoinette GUTIERREZ-CRESPIN, directeur chez Ernst & Young, et par Véronique HACCOUN, senior manager.

Antoinette GUTIERREZ-CRESPIN, *Directeur, Ligne de Services Fraudes et Investigation, Ernst & Young*

Je crois qu'Olivier a dressé un bon panorama des schémas que l'on peut trouver de manière récurrente sur la fraude. Moi, ce qui me frappe – dans ces dernières années je me suis véritablement intéressée au sujet et j'ai passé trois ans en Angleterre pour étudier tous les schémas, essayer de comprendre les typologies de fraudeurs, les profils psychologiques –c'est que le fraudeur est intelligent. Il est intelligent car il peut mettre en place des schémas complexes, cachés, difficiles à trouver.
La lutte observée en France contre la fraude et l'intérêt que l'on porte à ce fléau, sont également le fait de tous les pays. Dirigeants, responsables comptables et commerciaux sont d'autant plus intéressés par le sujet, que leur responsabilité pénale peut être mise en jeu. C'est pourquoi ils veulent mettre en place un maximum de procédures préventives pour se protéger contre des fraudeurs éventuels.
Quelques notions sur la fraude. Des études américaines montrent que les entreprises de ce pays perdent 5 % de leur revenu annuel à cause de la fraude, ces 5 % représentant 652 milliards de dollars. Je n'ai pas le chiffre correspondant pour la France. Il faut en moyenne dix-huit mois pour détecter une fraude, laps de temps au cours duquel le fraudeur peut s'organiser et récolter une bonne prébende. Tous les métiers, tous les secteurs sont concernés.

© IFACI

Je laisse la parole à Véronique.

Véronique HACCOUN, *Senior Manager, Ernst & Young*

Il est intéressant de noter qu'en France, en dépit des ravages causés par la fraude, il n'existe pas de définition légale de ce fléau.
La fraude est qualifiée selon trois natures de faits principaux : le détournement d'actifs (actifs financiers ou non financiers, liquides ou non liquides) ; les actions de corruption (aussi bien constituées des pots-de-vin que des avantages dissimulés ou de possibilité d'attraction, notamment de marchés, par différentes méthodes) ; la fraude aux états financiers. La fraude aux états financiers est certainement la plus rare ou la moins détectée aujourd'hui, même si l'on parle de plusieurs affaires dans l'actualité récente, mais elle coûte évidemment beaucoup plus cher qu'un détournement sur les stocks ou sur la caisse.
Il est inquiétant de constater que les fraudes sont aujourd'hui très largement combinées : on commence souvent par un acte comme un détournement d'actifs, qu'il faut ensuite dissimuler ; ce que l'on essaie de faire en camouflant quelques écritures comptables ; et puis on va essayer d'entraîner avec soi un trésorier ou un contrôleur de gestion, de manière à dissimuler l'ensemble du schéma et à opacifier les indicateurs. On passe ainsi, petit à petit, d'un événement spécifique (un détournement financier), à quelque chose de beaucoup plus large qui peut aller jusqu'à la présentation de faux bilans, avec des montants suffisamment inquiétants pour détruire la confiance des banquiers et des investisseurs.
La fraude est caractérisée par quatre éléments. 1) C'est toujours un acte intentionnel, jamais une erreur. 2) Il y a toujours une volonté de dissimulation. 3) La fraude se fait toujours contre un cadre de référence. Ce cadre de référence peut être la loi (la loi comptable, la loi du travail, la loi contre la concurrence, avec les éventuelles possibilités d'attribution de marchés de manière un peu exotique) ; il peut être aussi simplement les normes du groupe, qui préconisent par exemple que des acheteurs n'ont pas le droit d'avoir de relations spécifiques avec certains fournisseurs ou qui expliquent le mode de remboursement des notes de frais. Dès lors que le cadre est transgressé, on est déjà dans un acte de fraude. 4) Il y a toujours un avantage pour le fraudeur. L'avantage peut être direct, en espèces sonnantes et trébuchantes, ou indirect, par exemple par le biais de stock options ou de cession d'actions à des moments privilégiés.

On comprend alors l'importance que peuvent revêtir, au sein d'une entreprise, les dispositifs de prévention et la nécessité d'un contrôle interne très robuste.

Antoinette GUTIERREZ-CRESPIN

Le dispositif de prévention et de détection.
Comment faire pour mettre en place un certain nombre d'indicateurs et d'éléments protecteurs pour lutter contre la fraude ?
Notre expérience nous a appris que, compte tenu de la diversité des entreprises, de leur complexité, il n'existe pas de recette miracle, de check-list, de mode d'emploi garantissant contre l'action des fraudeurs.
Parmi les meilleures armes pour lutter contre la fraude, tout au moins la prévenir ou la détecter, il y a trois éléments majeurs : 1) le degré de conscience élevé, pour tout le monde y compris les auditeurs internes, de ce qu'est une fraude au sein de l'entreprise. 2) la connaissance de la réalité des implications d'une fraude (il faut pour cela sensibiliser l'ensemble du personnel à ce que l'on considère comme un comportement déviant). 3) la connaissance des facteurs et des indicateurs qui peuvent alerter sur la possibilité d'apparition ou d'existence d'une fraude ; en tant qu'auditeurs internes et externes, nous avons effectivement un rôle à jouer en aidant l'entreprise à mettre en place des indicateurs pouvant révéler les fraudes au moins les plus importantes.
Une fraude avérée soumet l'entreprise à une crise (au moins psychologique). Le traitement de la fraude, fait dans l'urgence et l'émotion, ne prend pas toujours la mesure des faits pour tirer les conséquences et mettre en place les mesures préventives qui s'imposent.
Quelles seraient-elles, ces mesures préventives ? Ce serait d'abord une charte d'éthique. Je disais tout à l'heure : il faut que tout le monde sache ce qu'est une fraude, ce qu'est un comportement déviant, et que ni

© IFACI

celle-là ni celui-ci ne peuvent être tolérés. Je donne un exemple : dans les grands codes d'éthique, on trouve de grandes idées sur l'éthique en général. Au niveau local, par exemple dans le département des fournisseurs, il faut mettre en place une charte d'éthique et s'assurer que tous les acheteurs adhèrent à cette charte, où il est expliqué, entres autres, qu'ils n'ont aucune relation personnelle, aucun conflit d'intérêt avec les personnes avec lesquelles ils sont en relation professionnelle, pour le bien de leur entreprise. C'est un code d'éthique concret, adapté au métier.

Le dispositif de prévention et de lutte passe par la sensibilisation et la responsabilisation de tous les acteurs de l'entreprise.

Véronique HACCOUN

C'est pourquoi il est extrêmement important de pouvoir définir qui fait quoi au sein des entreprises, qui a la responsabilité de tel domaine, de telle action, de manière à pouvoir déléguer des fonctions sans diluer les responsabilités et permettre un pilotage et un contrôle cohérents.
Il existe, en matière de prévention, des principes de base et des objectifs que vous connaissez. Ce sont : le respect du principe de séparation des tâches ; l'attribution des responsabilités et la clarification de l'organisation interne ; le contrôle de l'exercice des pouvoirs ; une prise de décision plus rapide et plus efficace ; une meilleure réactivité permettant une prise de décision au plus près des services demandeurs.
L'attribution des délégations doit se faire en fonction de différents critères : la situation géographique (proximité du délégataire) ; la situation technique (compétence) ; la situation hiérarchique (responsabilités liées au poste) ; le niveau d'activité (volume). Tout doit être mis en œuvre pour permettre et faciliter le fonctionnement courant de la structure, tout en préservant l'opportunité des contrôles.
La problématique est, sans préjudice de la responsabilité pénale des dirigeants, de faire comprendre à chaque manager responsable de son domaine, quelles sont les attentes, quels sont ses objectifs, et quels sont les pouvoirs dont il dispose. Il est important de définir, pour chacun, des objectifs réalistes et des modalités d'attribution qui lui permettent d'accepter ces objectifs.
Cela dit, on se rend compte que, même dans des sociétés qui aujourd'hui connaissent des croissances importantes, dans divers secteurs, certains de ces schémas n'existent pas. Par exemple, les signatures déposées en banque ne font pas toujours l'objet d'un suivi régulier, et des personnes mutées ou en retraite ont toujours leur signature déposée. Même chose pour les personnes habilitées à engager des dépenses. Dans ces domaines sensibles, la coordination et les procédures doivent être rigoureuses.

La compréhension et l'appréhension de la notion de fraude, nous l'avons dit, sont capitales, et le management doit donner l'exemple : on ne peut pas demander à des collaborateurs de respecter une certaine éthique, s'ils n'ont pas la conviction que leur direction fait de même. Les principes sont donc édictés pour tous. Ils doivent ensuite être déployés et peut-être adaptés en fonction des métiers. Les métiers de la finance, de la trésorerie, des achats doivent avoir sans doute leur propre charte d'éthique, une charte spécifique.
Pour appréhender la fraude de façon pragmatique, il faut connaître les éléments qui permettent de la qualifier en tant que telle. Il est important que ces éléments soient compris et assimilés par le management qui les présentera ensuite aux équipes.
Un diagnostic d'exposition au risque de fraude permet de mesurer la connaissance et l'état de préparation d'une entreprise sur la fraude, et plus précisément : de tester la compréhension des politiques et procédures anti-fraudes existantes ; de mesurer le degré de conscience des collaborateurs et de la conception qu'ils ont du rôle à jouer dans la lutte contre la fraude ; de mesurer la capacité de l'organisation à prévenir et détecter le risque de fraude, mais aussi à signaler et enquêter sur des fraudes soupçonnées ou avérées ; de s'assurer que les leçons ont été tirées des expériences des fraudes passées.
Il est évident que cette sensibilisation à la fraude doit être un élément de la culture de l'entreprise, mais cela prend du temps et suppose des moyens techniques et humains.
Outre l'environnement, la sensibilisation et la formation, la cartographie des risques de fraude est un outil indispensable.

 © IFACI

Antoinette GUTIERREZ-CRESPIN

La cartographie des risques, qu'est-ce que c'est ? C'est un dispositif qui permet d'identifier, à un instant T, la nature des risques de fraude qui menacent l'entreprise, compte tenu de ses processus, de son contrôle interne, et surtout de les hiérarchiser.
Le risque de fraude est un risque particulier qui nécessite une analyse spécifique. Cela veut dire que là où l'on identifie des risques forts, on doit mettre en place des contrôles, un processus de prévention adéquat ; enrichir le dispositif, et demander aux auditeurs internes de vérifier que le contrôle mis en place fonctionne bien. On voit là l'importance du rôle des auditeurs internes ou externes, dans la vérification de l'application des contrôles et de leur bon fonctionnement sur la partie fraude.
Nous allons faire maintenant quelques commentaires sur la partie fraude et systèmes d'information.

Véronique HACCOUN

Je ne suis pas une spécialiste des systèmes d'information, mais je vais essayer de vous exposer ma compréhension, et surtout notre expérience des systèmes d'information soit en tant qu'outil de traque de la fraude, soit en tant que vecteur de fraude. Aujourd'hui, dans les détections et les préventions de fraudes, le système d'information est un des outils clés, pour la mise en œuvre d'un contrôle interne efficace. En revanche, si le système d'information n'est pas utilisé convenablement, il peut être un vecteur de fraude extrêmement dévastateur pour l'ensemble de vos activités. L'aspect positif, c'est que le système d'information contient des informations précieuses lorsqu'on fait des investigations et des analyses.

Les risques de fraude existent via le système d'information lorsque l'une des étapes permettant de contrôler l'accès d'un utilisateur à une ressource informatique n'est pas correctement assurée. Ces risques sont notamment : l'usurpation de l'identité d'un utilisateur ; l'accès à des données non légitimes ; le passage de transactions non autorisées ; la modification ou la suppression directe des données. C'est pourquoi il est nécessaire de pratiquer des opérations de revue de sécurité au cours de la vie de l'application, comme les audits de configuration des composants (serveurs, bases de données) ; les tests d'intrusion ; la revue des habilitations ; l'audit des procédures de gestion.

En cas de suspicion de fraude ou de fraude avérée, un dispositif de détection doit être mis en place afin d'identifier les processus impactés et les types d'informations pour lesquels une analyse des données peut s'avérer pertinente. Il faut également extraire les données et procéder par itération pour confirmer ou non le processus de fraude et chiffrer le montant de la fraude.

Antoinette GUTIERREZ-CRESPIN

La dernière étape concerne l'investigation.
Avant chaque investigation, il nous semble important que le top management (ou le comité d'audit) soit systématiquement informé du caractère des fraudes, pour lesquelles des missions vont être diligentées. Ces missions doivent être conduites avec beaucoup de professionnalisme et d'expertise, que ce soit en interne ou en externe, et respecter la confidentialité.
Les indicateurs d'alerte sont divers : une dégradation des marges, des ratios d'endettement ; des hausses inexpliquées des achats ou de la masse salariale…
L'équipe chargée de l'enquête doit être capable d'identifier des faiblesses de contrôle interne ; de connaître les risques et les facteurs de risque liés aux activités ou aux processus concernés – c'est à mes yeux un élément majeur ; d'être en mesure de se faire assister par des experts internes ou externes sur les aspects IT, comptables, fiscaux et juridiques. Elle doit chercher à recouper l'ensemble des informations, s'assurer de leur cohérence et reconstituer le schéma de fraude du début à la fin, si possible, sachant qu'il y a souvent des entreprises externes qui viennent compliquer le cheminement.

© IFACI

Certaines investigations, si elles sont mal préparées ou mal conduites, peuvent générer des risques pour l'entreprise, comme la perte ou la disparition de preuves, voire l'impossibilité d'identifier les responsables ou de prouver leur implication dans des opérations frauduleuses.
Il est donc important de mettre en place une gestion de crise efficace, d'en décliner les grandes étapes et de la formaliser, à savoir : faire réaliser une investigation approfondie ; décomposer les mécanismes frauduleux ; évaluer les pertes subies ; collecter les pièces constitutives des dossiers.

Véronique HACCOUN

Comme vous vous en doutez, nous ne sommes pas en mesure (personne d'ailleurs ne l'est) de vous donner un mode d'emploi ou des recettes pour détecter ou mieux pour prévenir la fraude dans vos établissements.
Néanmoins, avec quelques idées et quelques principes de base, pas spécialement difficiles ou coûteux à mettre en place, vous pouvez disposer d'une assurance raisonnable sur un certain nombre de sujets. C'est ce que nous appelons **les douze règles d'or pour minimiser le risque de fraude**. Nous avons constaté que dans des entreprises importantes et reconnues, certaines de ces règles n'étaient pas appliquées, ou mal appliquées.

La première règle est la mise en place d'**un organigramme des responsabilités**, qu'on appelle aussi définition de postes. On se rend compte que, très souvent, des fraudes sont commises dans des structures où les responsabilités sont émiettées, diluées à un point tel que personne ne connaît l'impact de ses propres tâches sur celles des autres. Ce flou est extrêmement propice au développement de la fraude.
Un tableau des autorisations : ce sont les délégations de pouvoirs.
Une séparation des tâches raisonnable. Dans les entreprises que vous représentez, je présume que les tailles critiques sont atteintes pour assurer une séparation des tâches. Dans les PME de dix, quinze personnes, le comptable fait les remises en banque, les enregistrements comptables, et c'est lui le trésorier. C'est inévitable, mais il faut mettre en place les contrôles adéquats.
Une gestion des habilitations d'accès aux fichiers : qui peut faire quoi, en consultation, en modification.
Des outils standards de sécurité informatique. Est-il normal de conserver, comme nous l'avons constaté, des périodes comptables ouvertes pendant plus de six mois, avec la possibilité de modifier des écritures ? Est-il normal que des systèmes de gestion et des systèmes comptables ne concordant pas, ne provoquent pas d'état d'exception, de remontée d'anomalie ?
Une transparence des informations suffisante.
Un contrôle systématique des entrées sur les fichiers informatiques sensibles, notamment les fichiers paye et trésorerie.
Une supervision hiérarchique formelle. Il faut revenir aux bons principes de base de l'audit : en période de clôture, trimestriellement, semestriellement ou annuellement, quelqu'un doit superviser la manière dont les analyses des décomptes et la restitution des informations ont été faites ; quels sont les fichiers source ? Ont-ils été convenablement analysés ?, etc. Il y a dans ces domaines des potentialités de pertes de contrôle très propices à la réalisation de fraudes.
Un ajustement des grands équilibres comptables. On revient sur les indicateurs clés : y a-t-il des raisons spécifiques, rationnelles et rationalisées de la détérioration de la marge, des cash-flows, de la perte sur un certain nombre de business units ou, à l'inverse, est-il normal que, d'un coup, la masse salariale ait fortement augmenté ?
Une sensibilisation du personnel au trafic d'influence. Que représente-t-il en termes d'impact sur l'image et donc pour la pérennité de l'entreprise ?
Une sensibilisation du personnel au conflit d'intérêts. Il faut expliquer à l'ensemble du personnel, via des chartes d'éthique, des livrets d'accueil, des formations régulièrement dispensées, ce que sont les conflits d'intérêt.
Une rotation suffisante des personnels des postes sensibles. C'est plus facile à dire qu'à faire, en France surtout. Mais il faut essayer, car c'est un point très important, notamment pour les postes-clés.

© IFACI

Antoinette GUTIERREZ-CRESPIN

En conclusion, je voudrais ajouter que les fraudes les plus récentes que j'ai pu observer et qui ont coûté très cher, à la fois en termes de réputation et de dommages directs, concernaient des petites filiales de sociétés cotées, soumises à SOX, et qui étaient passées au travers des mailles du filet. Ce qui prouve 1) que ce n'est pas parce qu'une entreprise est SOX qu'elle échappe au risque de fraude, 2) que les petites filiales passent plus facilement au travers du maillage de l'analyse détaillée, du contrôle interne, des délégations de pouvoir, des autorisations, etc., et ce quel que soit le pays. Quand il y a des investissements à l'étranger, toute la problématique de corruption prend un intérêt particulier.

QUESTIONS

Jean-Luc MASSELIN

J'ai noté que vous avez évoqué la notion de délégation de pouvoirs pour segmenter ou répartir les prises de risque au sein d'une société ou d'un groupe. J'ai compris qu'il y avait un certain nombre de méthodes ou de modalités à respecter pour que cela fonctionne bien.
Quand on aborde ce genre d'organisation, des questions se posent, notamment sur la robustesse de ce système avec les dispositifs de contrôle et de *reporting* qui peuvent exister, certains considérant que, s'il y a un exercice par trop pressant et documenté, rapportant jusqu'aux plus hautes sphères les observations faites, les délégations à ce moment-là tombent, puisqu'il y a information et que le manager suprême est informé.
Cela pose pratiquement un problème sur l'organisation du contrôle, notamment pour des auditeurs internes qui ont vocation à rendre compte à la direction générale et au comité d'audit, et des problématiques juridiques et pratiques assez complexes.
Qu'en pensez-vous ?

Véronique HACCOUN

Je pense que vous avez raison. Ce qui est certain, c'est que si ces délégations de pouvoir n'existent pas, il est difficile de déterminer les zones de responsabilité.
Il existe un contrat qui entérine un dispositif de manière formelle, et puis les faits qui peuvent le contrecarrer. Souvent, dans les organisations, il y a à la fois un supérieur hiérarchique et un supérieur fonctionnel.
C'est certainement difficile, mais il faut faire en sorte que les protocoles de communication et les délégations de pouvoir soient en ligne avec les responsabilités fonctionnelles. Si on se rend compte qu'il y a un décalage entre ces responsabilités et la réalisation dans les faits, c'est que probablement on est dans une situation problématique. C'est la raison pour laquelle il est nécessaire de faire réviser ces délégations de pouvoir, et de voir dans quelle mesure elles sont réellement portées dans les faits.
Mais je suis d'accord avec vous que l'on peut aboutir à des situations très enchevêtrées. Nous avons vu le cas, il n'y a pas très longtemps, d'un directeur financier, censé rapporter à son directeur du contrôle de gestion, et qui communiquait en direct avec le PDG, ce qui interdisait au directeur du contrôle de gestion d'apprécier et le contrôle et les réalisations. Ce sont des situations extrêmement compliquées.
Du point de vue juridique, on se heurte sans doute à des situations où l'on est en plein conflit. Mais là, on est dans une zone qui normalement montre l'échec et l'insuffisance des protocoles de communication.

© IFACI

Liens entre les mécanismes de montage de fraude et les mécanismes de blanchiment

Noël PONS

Nous allons poursuivre avec Raoul d'ESTAINTOT, responsable de la cellule prévention des fraudes au Crédit Mutuel. Il va nous expliquer quels sont les liens entre les mécanismes de fraude et les mécanismes de blanchiment.

Raoul d'ESTAINTOT, *Responsable Cellule Prévention des Fraudes, Crédit Mutuel*

Dans un premier temps, nous allons réfléchir sur la notion de fraude et de blanchiment, puis dans un deuxième temps j'essayerai d'illustrer mes propos par quelques exemples, avant de terminer par la mise en évidence de ces liens entre les mécanismes de fraude et de blanchiment.

Travaillant dans une banque, je me positionnerai dans un contexte surtout bancaire. Le comité de Bâle, qui rassemble les principales banques centrales et qui a une initiative très importante en matière de réglementation prudentielle, a été amené à réfléchir sur la notion de fraude avec le risque opérationnel. Le comité de Bâle définit le risque opérationnel comme étant « un risque de perte dû à des personnes, processus ou systèmes inadéquats ou défaillants, ou résultant d'événements extérieurs ». Le comité de Bâle donne sept types de risques opérationnels ; parmi ces sept, j'en retiens trois qui concernent directement la fraude.

D'abord **la fraude interne**, par exemple des informations inexactes sur des positions ; les vols commis par un employé, les détournements ; les délits d'initié, c'est-à-dire l'utilisation par un collaborateur d'une information confidentielle, qui va être utilisée sur les marchés pour acheter ou vendre des titres avant une annonce importante, qui aura une incidence sur l'évolution du titre, et procurera un gain substantiel au collaborateur.

Le deuxième type de risque opérationnel défini par le comité de Bâle est **la fraude externe**. Ce sont les hold-up, les faux en écriture, les chèques de cavalerie, et les dommages dus au piratage informatique, autrement dit les fraudes informatiques.

Le troisième type de risque, ce sont **les pratiques concernant les clients, les produits et l'activité commerciale,** par exemple l'utilisation frauduleuse d'informations confidentielles sur la clientèle, des opérations boursières malhonnêtes dans le but d'enrichir l'établissement et… le blanchiment d'argent. **Le comité de Bâle cite le blanchiment d'argent dans les fraudes.**

Le code pénal (dans son article 324-1) donne une définition du blanchiment en deux paragraphes : le premier concerne le client, le deuxième, le banquier. Le premier dit que *« le blanchiment est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect. »* Le deuxième paragraphe dit : *« c'est le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit. »*
Le blanchiment, on le voit, est la dissimulation de l'origine frauduleuse des capitaux ; il y a, en amont, une fraude, un délit qui a généré des fonds, et ce qui est important pour un fraudeur, ce n'est pas de frauder pour frauder, mais de frauder pour obtenir de l'argent et de pouvoir utiliser cet argent obtenu frauduleusement. Le blanchiment est un processus dynamique qui va impacter d'une façon générale les activités financières.
Le GAFI décrit le blanchiment en trois phases. La première phase est le placement. Le placement a pour objet de transférer, dans la vie économique légale, les espèces procurées par la commission d'un acte délictuel (exemple : le trafic de stupéfiants). Les banques sont un vecteur important par le biais des comptes de tiers.

 © IFACI

Mais la préoccupation du délinquant va être de mettre un maximum d'espace entre la commission de l'acte délictuel et lui-même, afin d'éviter que des tiers (banquiers, services de poursuite de justice, de répression) ne remontent non seulement à la commission de l'acte délictuel en question, mais aussi à l'auteur de cet acte.
C'est là que commence la deuxième phase, dite d'empilage, où, par différents mécanismes : des transferts (notamment à l'étranger), la mise en place et l'utilisation de certaines sociétés (sociétés taxis, sociétés qui n'ont pas d'existence légale, sociétés fantômes, sociétés qui ont une existence légale mais pas d'activité commerciale, sociétés où l'on va mélanger des flux d'argent sale avec des flux propres) , le fraudeur va essayer de mettre cette distance entre l'origine des fonds et lui-même.
La dernière phase est la phase d'intégration : les fonds ont été blanchis, et le délinquant va pouvoir les utiliser sans que l'on puisse remonter à lui et à l'acte délictuel qui a généré les capitaux.
On commence à voir là des liens entre fraude et blanchiment, le blanchiment étant en fait un délit de conséquence, puisqu'il est nécessaire qu'en amont un délit ait été commis. On pourrait simplifier en disant que la fraude, c'est de l'argent qui s'en va, notamment dans la banque, c'est un trou dans les comptes de la clientèle ou dans les comptes de la banque, qui va impacter les emplois, les actifs de la banque. Le blanchiment, ce sont des ressources suspectes, qui vont impacter les ressources, passifs de la banque ou de clients, c'est-à-dire les crédits aux comptes de nos clientèles.

Il existe une décision juridictionnelle très importante de la Commission bancaire, qui date de 2002, et qui précise que les opérations de blanchiment *« ne sont pas uniquement celles par lesquelles des sommes sont versées au crédit d'un compte, mais également celles par lesquelles des sommes sont retirées de ce compte ».*
Le soupçon peut donc aussi bien concerner les opérations de sortie que les opérations d'entrée de fonds. Il y a bien là un lien à faire entre blanchiment et fraude.
Les banques sont tenues de déclarer à TRACFIN les opérations suspectes, susceptibles d'être du blanchiment.
Mais la troisième directive européenne, qui doit entrer en vigueur avant le 15 décembre 2007, élargit considérablement le périmètre de la déclaration de soupçon : tout soupçon d'une fraude financière quelconque, dès lors qu'elle génère des fonds, doit faire l'objet d'une déclaration à TRACFIN. On constate que les périmètres de la déclaration de soupçon et du délit de blanchiment deviennent identiques.

Il y a incontestablement des liens entre fraude et blanchiment : fraude et blanchiment sont les deux côtés d'une même médaille. Le blanchiment est la dissimulation de l'origine frauduleuse des fonds. Mais si, d'après le Code monétaire et financier, quatorze catégories de professionnels sont assujetties à la prévention du blanchiment, la répression du blanchiment et des délits financiers s'applique à tout le monde (par exemple au directeur financier d'une entreprise).
Les moyens utilisés par les délinquants, blanchisseurs ou fraudeurs, sont de façon générale identique. Il y a une volonté de dissimuler, et pour dissimuler, il y a recours aux faux : cartes d'identité, justificatifs de revenus, bulletins de salaire, factures, etc. Il y a l'anti datage, pour dissimuler les anachronismes. Il y a l'absence ou la fausse justification des opérations. Il y a la rupture de la traçabilité des opérations.

La démarche de prévention contre la fraude et le blanchiment est la même. C'est d'abord une faculté d'étonnement constante : pourquoi telle situation, tel mouvement, telle écriture ? Quelle est l'origine des fonds, leur destination ? Quelles sont les justifications ?
Quelles sont les parades ? Une des grandes règles en matière de lutte contre le blanchiment, c'est de connaître ses clients *(Know Your Customers)*. Mais c'est aussi de connaître ses collaborateurs (ceux qui sont très endettés) ; ses fournisseurs ; ses dirigeants (voir Enron).
Une autre règle est que les opérations, de façon générale, doivent être en cohérence avec le profil de la contrepartie. Pour les entrées en relation, nous demandons à nos collaborateurs, outre les obligations d'identification – qui sont de plus en plus lourdes –, de dresser un profil de fonctionnement du compte et un profil du client en question par rapport au risque de blanchiment : de nombreuses opérations avec l'international, de même que des opérations débitrices importantes et répétées, par exemple, sur le compte d'une personne âgée, doivent susciter des questions.
Autre règle encore : les opérations, d'une façon générale, doivent être tracées. On doit connaître l'origine et la

© IFACI

destination géographique ; l'identification du donneur d'ordre et du bénéficiaire.
Les opérations doivent être causées, justifiées.
Les liens entre fraude et blanchiment peuvent être illustrés au travers de mécanismes comme la carambouille, la cavalerie et la fraude à la TVA intra-communautaire (carrousel).

En conclusion, la mise en œuvre de diligences permet aussi de veiller au respect des mesures restrictives prises à l'encontre de certaines personnes ou de certains pays, les embargos par exemple.
Tout le monde est concerné par la sécurité financière, qu'il s'agisse de lutte contre les fraudes, de financement du terrorisme, de blanchiment d'argent sale, ou du respect des embargos, dès lors que l'on dispose d'une comptabilité ou d'un compte bancaire, vecteurs propices à tous les types de détournements.

Comment intégrer des modules de prévention de la fraude dans la gestion de projets ?

Noël PONS

Nous allons poursuivre avec une entrée, une plongée dans l'information, avec Philippe TROUCHAUD et François VIDAUX.

Philippe TROUCHAUD, ***Associé, PricewaterhouseCoopers***

Je vais vous parler des différentes natures d'outils dont on peut se servir pour essayer d'identifier des fraudes, et je vous donnerai les grands principes qu'il faut respecter pour mettre en œuvre des outils qui permettent de déceler des fraudes de façon efficace.

On observe, en général, qu'une fraude est une accumulation de petits détournements. Cela veut dire qu'on a rarement vu quelqu'un sortir d'une entreprise avec deux millions d'euro dans la poche.
La caractéristique des petites fraudes, celles qui sont le plus préjudiciable à l'entreprise, c'est l'accumulation. Ce peut être la fraude d'un salarié qui force un peu, pendant des années, sur les notes de frais : j'ai ainsi découvert une personne qui avait détourné 14 000 euros sous forme de notes de frais.
Qu'est-ce que cela veut dire ? Cela veut dire que ces fraudes-là font nécessairement appel au système informatique, et qu'elles impliquent une défaillance du système d'information : c'est quelqu'un qui a un accès qu'il ne devrait pas avoir, que ce soit un comptable qui peut créer un fournisseur, modifier un rapprochement bancaire, ou bien un informaticien qui a compris le contenu fonctionnel d'une base de données. Pour déceler ce genre de fraude, on ne peut pas se baser sur le dispositif de contrôle interne, tout simplement parce que la fraude a pu se concrétiser à cause d'un dysfonctionnement du contrôle interne. Tout cela pour dire que, quelle que soit la qualité de vos procédures de contrôle interne, si vous souhaitez déceler des fraudes répétitives, il vous faut des outils de détection. Si l'on prend l'exemple du monde bancaire, où des centaines, voire des milliers d'agences traitent des milliards de transactions, vous ne pouvez pas découvrir de fraude sans un outil informatique.

Il existe différents types d'outil. Tout d'abord les procédures de contrôle manuelles : on arrive inopinément dans un magasin, dans une agence, et on contrôle physiquement un certain nombre de pièces comptables. Compte tenu de la complexification des mécanismes de fraude, je suis très sceptique sur la probabilité, sauf coup de chance, de découvrir des fraudes avec ces méthodes.
Ensuite, il y a des outils un peu frustes, qui sont les outils de filtrage. Grosso modo, on définit les requêtes, on recherche des règlements supérieurs à un certain montant, et l'on obtient une information brute. Mais il

© IFACI

reste tout un travail d'exploration à faire. C'est un outil qui nécessite beaucoup de travail manuel pour éventuellement déceler des fraudes.
Les moteurs à base de règle permettent de mettre en œuvre des algorithmes. Exemple : au lieu de rechercher tous les paiements supérieurs à 1 000 euros, on recherchera les paiements supérieurs à 1 000 euros et domiciliés à l'étranger. Les requêtes peuvent être beaucoup plus sophistiquées que dans cet exemple.
Passons aux produits dits analytiques. On met en action dans ces outils ce que l'on appelle des mécanismes de recherche de régression non linéaire. Ce sont des algorithmes (Benford, par exemple). Ces outils, à partir des données, signalent non pas des schémas de fraude, mais des corrélations de plusieurs données qui paraissent bizarres, des cas potentiellement anormaux, sur lesquels, de toutes façons, il faut faire des recherches. Ces outils sont très performants quand il y a des seuils de contrôle. Ils sont très efficaces lorsque les transactions sont nombreuses, mais ils ne sont pas faciles à mettre en œuvre.
Enfin, il y a les systèmes intelligents (que l'on voit encore assez peu sur le marché), qui font appel au concept d'intelligence artificielle en informatique et aux systèmes à base de réseaux de neurones ; ce sont des systèmes qui se basent sur un certain nombre d'algorithmes, et qui sont capables de « comprendre » un cas atypique et de l'intégrer dans leurs propres recherches.
Si vous lancez un projet ou si vous voulez améliorer vos outils d'analyse existants, il faut bien prendre en compte le cycle de vie d'une information. Une information se crée, elle se maintient, elle s'analyse, elle se reporte et elle s'archive. Très souvent, les outils que l'on met en service se limitent à l'analyse, et ils oublient que quelqu'un peut créer une information, un compte fournisseur…

Prenons le cas d'un système de gestion des achats qui est raccordé, interfacé avec la comptabilité. Dans 99,9 % des cas, il y a une commande, une livraison, un paiement. Mais certains achats ne font pas l'objet d'une commande : les abonnements, les loyers ; les achats dits de la présidence, comme le sponsoring. Il existe donc un mécanisme dit de commande ouverte, qui ne requiert pas un compte fournisseur ; et il y aura toujours un petit malin qui va s'engouffrer dans cette brèche. Il faut donc bien comprendre où sont les données, comment elles sont gérées, mais aussi quels sont les mécanismes qui permettent de contourner les cas généraux.
Beaucoup de fraudes se font aussi sur la base d'un fournisseur fictif. On constate très souvent, que dans l'entreprise, jamais, au-delà de la création, personne ne vérifie la qualité des comptes fournisseurs créés. Il est possible aussi de créer un fournisseur en modifiant le nom d'un fournisseur existant (par exemple en rajoutant ou en supprimant une lettre). Toutes les possibilités de fraude se cachent dans le détail.
Je voudrais citer la norme SAS 99 qui impose aux auditeurs de vérifier la gestion des *over day*, pour s'assurer que toutes les opérations, passées un week-end ou à des heures indues, sont dûment autorisées. Nous avons 4 000 collaborateurs en France ; chaque année, nous faisons ce genre de contrôle, et chaque année nous en prenons un ou deux qui ont été suffisamment bêtes pour saisir des frais un dimanche. Et quand on trouve un exemple comme celui-là, généralement, la nouvelle se répand vite dans l'entreprise. C'est pourquoi j'insiste sur le fait que la médiatisation du contrôle permet de réduire considérablement le risque de fraude.
Les factures fournisseurs, notamment des consultants indépendants en informatique, peuvent donner lieu à des manipulations : le consultant demande 600 €/jour ; le responsable du service lui donne 700 €/jour et se fait « rembourser » 100 € en espèces. Un prestataire externe est recruté comme ingénieur systèmes pour déceler des fraudes ; en réalité il n'a qu'un BTS. Vous imaginez où passe le différentiel. Ce ne sont pas des cas d'école mais des cas vécus.

Voilà le genre de fraudes que l'on peut détecter avec de bons outils. J'ai cité tout à l'heure les seuils de contrôle. Utilisez ces seuils, et vous découvrirez toujours une dispersion autour du seuil. Cela ne veut pas dire qu'il y a systématiquement fraude, mais cela peut signifier quelque chose, et devrait vous conduire à faire évoluer votre dispositif de contrôle interne.

Noël PONS

J'accueille maintenant François VIDAUX qui va nous parler des modules d'intégration de la fraude.

François VIDAUX, *Consultant, Exos*

Effectivement je vais vous dire comment intégrer des modules de prévention de la fraude dans la gestion de projets.

Un certain nombre de questions se posent : quand doit-on intégrer des modules de prévention ? L'auditeur interne doit-il ou non y participer ? Si oui, à quel moment doit-il intervenir ? Quelles solutions seront-elles retenues (développement, ERP) ?
L'audit – selon moi, bien entendu – n'a qu'un simple rôle de conseil dans la gestion des projets. En revanche, il peut être l'aiguillon dans la gestion des systèmes d'information et prévoir un certain nombre de règles, comme la traçabilité des opérations (la piste d'audit).
Dans la gestion des projets, l'aspect intégration des modules de prévention de la fraude va se concrétiser à partir d'un certain nombre d'organes comme la gestion des risques, si elle existe, les cellules de gestion de la fraude, quand elles existent également, le contrôle interne, et éventuellement d'autres organismes préexistants ou pas dans l'entreprise.

Quelles sont les étapes d'un projet ?
A quel moment peut-on introduire ou penser à des modules de prévention de la fraude : a priori ou a posteriori ? Selon moi, il faut y penser dès la conception du cahier des charges, avant la phase de réalisation technique. Prenons l'exemple de projets avec des protocoles Internet. Dès l'établissement du cahier des charges, il va falloir penser aux moyens de se garantir contre les intrusions, internes ou externes. Et tout au long des opérations de conception des applications il faudra réfléchir à la mise en place de modules a priori, a posteriori. Un élément est particulièrement important dans la préparation des modules de détection ou de prévention de la fraude, c'est l'analyse des incidents.
Autre élément important, les tables de paramètres (ou tables de références). Comment mettre sous clé ces tables ? Prenons la paye par exemple : certains paramètres sont très sensibles (plafond sécurité sociale, taux de charge…), et sont autant de portes d'entrée à des mécanismes de fraude.
Sur ces aspects, il faut être extrêmement vigilant dès, et même avant, la livraison, la mise en production des applications, en n'oubliant pas qu'il faut toujours une séparation extrêmement stricte entre les différents environnements : l'environnement études, l'environnement tests intégration et l'environnement de production ; ces séparations de fonctions doivent être mises en place au fur et à mesure, avant la livraison des applications, c'est-à-dire avant leur mise en production.

Première étape.
Comment s'inscrit ce projet dans l'ensemble des processus de l'entité ? Y a-t-il des liens avec d'autres projets préexistants ou d'autres projets qui vont être développés ? Quelles sont les règles du jeu, c'est-à-dire quelles sont les informations qui vont circuler, quelles sont celles qui vont alimenter ou qui vont être reçues des bases de données relationnelles ? Tous ces points-là vont devoir être analysés systématiquement.
Il faut utiliser une cartographie des risques pour déterminer la sensibilité des secteurs d'activité. On entend beaucoup de choses sur la cartographie des risques. Malheureusement, on constate bien souvent que cette cartographie des risques est relativement limitée. Il vaut mieux creuser une catégorie de risques particulière plutôt que d'essayer de prendre en compte tous les risques de l'entreprise. Mais tout est fonction de la taille de l'entreprise.
Il ne faut pas oublier qu'un projet, c'est aussi des changements, des modifications, des mises à jour. Bien souvent, on a en tête, au début, le projet développé, et l'on perd un peu sa trace, au fur et à mesure des évolutions. Il faut tenir compte de toutes les mises à niveau.

Deuxième étape.
Les travaux préalables doivent inclure le recensement des données particulièrement sensibles. Ce n'est pas une opération facile, parce que les données sensibles varient en fonction des secteurs d'activité (banque, industrie, commerce…). Il faut les sérier, les trier, et déterminer celles à surveiller particulièrement, a priori

 © IFACI

(contrôle interne) ou a posteriori (audit interne ou externe).
Il faut également prévoir les extractions de données structurées qui seront exploitées par le contrôle interne, le secteur *risk management* ou d'autres secteurs de contrôle, a priori et a posteriori. La plupart du temps, celles qui sont extraites a priori sont plus volumineuses, parce que la mission à accomplir est plus longue ; celles qui le sont a posteriori sont moins nombreuses et éventuellement beaucoup plus fines à l'analyse.

Troisième étape.
Cette étape consiste à proposer des modules de prévention de la fraude à intégrer dans les applications, ou autres *softwares* et progiciels. Citons, à titre d'exemple : une analyse automatique des doublons, des trous, des RIB (comptes joints, comptes identiques, adresses, etc.), des rejets, des incidents ; des prévisions de logs à communiquer aux divers services de contrôle et à l'audit, etc.

Le rôle de l'audit.
Les résultats des extractions et analyses intégrées dans les applications et autres *softwares* sont destinés aux secteurs contrôle interne et *risk management*, et, bien entendu, à tous les secteurs qui traitent de la fraude. L'audit doit bénéficier des travaux récurrents effectués par les autres secteurs.
Il va également utiliser l'univers d'audit, c'est-à-dire un ensemble de tables constitué à partir de l'univers de l'entreprise dont il ne conservera que les parties de tables nécessaires aux extractions, auxquelles viendront s'ajouter des outils internes préexistants dans l'entreprise (type BO, ACL, IDEA, etc.).Il construira donc ses requêtes à partir de ces outils, et chaque fois qu'une application (ou un progiciel) sera mise en place, l'univers d'audit sera mis à jour pour faire les analyses a priori ou a posteriori. J'insiste particulièrement sur l'univers d'audit qui souvent, malheureusement, n'est pas constitué. On n'approche pas suffisamment les tables, parce que les systèmes d'information font encore un peu peur.

Noël PONS

Je redonne la parole à Philippe qui va nous parler des problématiques de *datamining*.

Philippe TROUCHAUD

Je vais prendre une image : la difficulté de ces outils, dans le paramétrage, c'est celle que rencontre le chercheur d'or : si vous tamisez trop large, vous ne retenez rien ; si vous tamisez trop fin, vous êtes submergé de travail.
Il y a, dans la mise en œuvre d'un outil quel qu'il soit, une phase d'apprentissage pour l'entreprise, de l'outil et de son maillage. C'est le point clé pour le rendre réellement opérationnel, parce que si vous relevez trop d'exceptions, vous n'aurez pas le temps de les traiter ; si vous n'en relevez pas, cela veut dire que votre outil n'est pas opérationnel.
Je n'ai pas de recette miracle à vous donner. Je soulignerai simplement le fait que ces outils doivent pouvoir évoluer très facilement, parce que les cas de fraude évoluent, parce que vos systèmes évoluent, vos produits et la façon dont vous gérez vos fournisseurs également.
Un dernier point : la mise en œuvre de ces outils requiert des compétences dans la statistique, le *datamining*, les systèmes d'information, et une connaissance des mécanismes de la fraude. Les personnes capables de mettre au point de tels outils ne sont donc pas légion. Lorsqu'elles quittent l'entreprise, on ne trouve plus personne qui soit capable de maintenir et de faire évoluer l'outil, et rapidement on se trouve devant une usine à gaz à laquelle plus personne ne comprend rien. C'est pourquoi, il faut faire en sorte que plusieurs personnes connaissent cet outil en profondeur.
Il n'est pas réaliste non plus de vouloir tout documenter (comme le préconisent les auditeurs), parce que, encore une fois, cet outil, pour être efficace et pertinent en termes d'assistance à l'identification de fraude, se doit d'évoluer pratiquement tous les jours. Il faut donc trouver des équipes réduites qui le maîtrisent parfaitement.

© IFACI

QUESTION

Question

Il y a un modèle logique qui est assez plaisant : on conçoit bien, on prévoit, on organise et bien évidemment tous les développements informatiques respectent toutes ces étapes. On a doublé les compétences clés, on a correctement documenté. On a besoin d'un univers d'audit qui couvre tous les aspects de l'activité, donc on doit avoir accès à tout.
Avez-vous le sentiment qu'aujourd'hui on progresse vers une meilleure maîtrise ou que finalement, on a bien les clés, mais on n'y arrive pas ?

Philippe TROUCHAUD

Je pense que chacun peut apporter sa réponse. Pour moi, on est encore très loin d'une maîtrise parfaite. J'observe une sensibilité accrue des dirigeants au phénomène de la fraude, et, dans le même temps, je constate que dans la plupart des cas, les entreprises ont des outils de recherche de fraude très frustes, voire pas d'outils du tout et pas du tout de moyens.
Or les mécanismes de fraude deviennent de plus en plus complexes, parce qu'ils s'accompagnent d'une dématérialisation des flux, d'*outsourcing*, de *share services*. J'ai en mémoire une entreprise qui avait complètement perdu la maîtrise de ses flux de paiement, au point qu'elle ne savait plus qui créait des comptes bancaires. Elle s'est aperçue que des personnes externes à l'entreprise avaient la possibilité de créer des comptes bancaires pour leur compte.
Donc, pour répondre à votre question, nous n'avons pas la maîtrise complète des outils. Je vous ai indiqué ce qu'il faudrait faire, mais avant tout, il faudrait convaincre vos dirigeants que c'est réellement là qu'il faut mettre des moyens.

François VIDAUX

Effectivement, je suis tout à fait d'accord avec ce que vous avez dit : on peut toujours faire des vœux pieux. Je vous ai parlé d'univers d'audit et de tables, mais tout dépend de l'environnement dans lequel on se trouve. Si l'on évolue au milieu de centaines d'applications, de milliers de programmes, il n'est pas évident de savoir sur quelle table porter son attention, parce qu'il y a des imbrications, des règles du jeu différentes, des techniques différentes. C'est bien d'avoir des outils, mais les outils ne feront que ce que vous leur demanderez.
Je crois qu'il faut être modeste, et beaucoup de progrès restent à réaliser avant que les auditeurs disposent de toutes les informations sur leur poste de travail, de leur univers d'audit, de leur serveur particulier et, sur ce serveur, de toutes les tables nécessaires.

© IFACI

Comment un auditeur peut-il identifier le risque de corruption privée dans l'entreprise ?

Noël PONS

En 1956 ou 1958, Maurice Rolland, président de la Cour de cassation, disait que la fraude, c'était avant tout l'homme. Quel que soit le système informatique que vous mettez en place, quelqu'un peut utiliser ce système, le manipuler, ou l'organiser. Quel que soit le montage (primaire ou extrêmement sophistiqué), il faut, pour le découvrir, utiliser son flair, sa connaissance, son expérience, et garder une capacité d'étonnement.
En fait, traquer la fraude est un véritable métier. Il y faut de la constance et un moral d'acier, mais c'est un domaine où l'on ne s'ennuie pas. C'est un domaine où, que l'on soit confronté à des fraudeurs primaires ou à des fraudeurs professionnels, il y a toujours quelque chose d'intéressant à découvrir et à apprendre.
Le problème, c'est que tous les pays n'axent pas leurs efforts et leurs recherches dans la même direction.
J'espère quand même qu'au cours de cette matinée, vous aurez glané des informations intéressantes, et qui vous permettront de régler certains problèmes.

Nous allons maintenant travailler sur un des sujets les plus complexes qui soient. Complexe de par le montage professionnel, organisé, structuré. Et il faut, à partir des comptes, chercher et reconstituer ce montage.
Comment un auditeur peut-il identifier le risque de corruption privée (ou le risque de corruption en général), dans l'entreprise ? Pourquoi corruption privée ? Parce que, depuis 2005, il y a une loi (qui a fait beaucoup de bruit) qui réprime le délit de corruption privée.
Le délit de corruption publique est connu : c'est un agent public qui, à un moment donné, touche de l'argent d'une entreprise. Désormais, à la suite des nouveaux textes émis par l'OCDE, le secteur privé n'est plus à l'abri du délit de corruption et de ses sanctions, lesquelles sont plus importantes. Si un directeur des achats se fait payer par son fournisseur, il ne sera plus renvoyé pour motifs administratifs ou pour escroquerie ou détournement ; il sera passible de l'accusation de corruption avec tout ce que cela implique, y compris l'impact sur l'image.
Nous allons entrer dans un schéma un peu compliqué, **avec deux types de recherche : l'identification des preuves directes et l'identification des preuves indirectes.** Les preuves directes, à partir des postes cadeaux et des relations publiques. Les preuves indirectes, plus complexes, en développant une analyse transversale.

Les preuves directes : elles peuvent être données par l'analyse des postes de charges, et leurs variations éventuelles. Par exemple, dernièrement, dans une entreprise du secteur privé, on a trouvé dans le poste cadeaux dix-sept manteaux de fourrure et cent quarante paires de chaussures, ce qui peut inciter à faire quelques recherches !
Mais si le fraudeur a un peu de cervelle, il ne laissera pas ces charges dans les comptes de cadeaux : il les noiera dans une structure, selon trois méthodes classiques, vieilles comme les fraudes. Soit il sous-traitera ces financements à une structure en principe non filialisée, mais liée à l'opération. Soit il noiera ces factures dans un compte de charges générales. Soit encore il regroupera les fausses factures chez un prestataire tiers, le plus souvent en fin de mois. Soit enfin le paiement se fera en espèces à partir d'une caisse noire : c'est une vieille méthode, où sont très performantes les régies publicitaires qui sont un système de blanchiment à elles seules.
Vous voyez que, dans les preuves directes, vous disposez d'éléments de contrôle, lesquels seront pertinents dans la mesure où les fraudeurs n'auront pas eu le temps d'organiser et de structurer leur système.

Les preuves indirectes : dans ce cas l'auditeur a un soupçon mais ne dispose pas d'indicateur. Comment reconstituer le cheminement frauduleux ? D'abord en analysant les projets en portefeuille : on peut trouver des indices de fausses factures ; en identifiant la manipulation des offres (offre complexe déposée avant la date d'échéance) ou la manipulation des prestations (facturations complémentaires) ; en analysant les opérations

© IFACI

contentieuses : beaucoup de fraudes, du moins lorsqu'elles sont techniquement bien organisées, se terminent par des contentieux, grâce auxquels l'argent est transféré.

Quels sont les indicateurs les plus probants ?
Le même fournisseur est souvent présent. La réalisation des marchés est le fait de sous-traitants, avec telle collectivité, telle entreprise. On se trouve là avec une problématique de travail clandestin, de fausses factures et de manipulation.
Les marchés perdurent sans cohérence : théoriquement le marché devrait être fini, or on continue à facturer.
Les opérations de fractionnement : on casse l'opération pour qu'elle ne soit pas lisible.
Les marchés à forte marge : un fournisseur X bénéficie de tous les marchés à très forte marge, alors que les autres ont des marchés à marge beaucoup plus restreinte.

Dans toutes ces opérations, les structures extérieures (TRACFIN, les commissaires aux comptes…) sont très impliquées, et ne travaillent peut-être pas dans le même sens, mais sur le même domaine. Il serait bon qu'elles travaillent toutes dans le même sens, car cela faciliterait le travail et permettrait peut-être de limiter ces risques importants.

QUESTION

Question

Quand j'ai le sentiment, au travers des investigations que j'ai faites, d'être dans une situation de fraude effective ou de corruption effective, quelle est la limite, en investigation privée dans une entreprise, de ce que l'on peut faire ou ne pas faire, et quelle est la bonne logique d'articulation avec d'autres acteurs ?

Noël PONS

L'investigation privée que vous ne pouvez pas faire, c'est tout ce que l'on appelle en anglais *due diligence* sur les personnes. Vous ne pouvez pas envisager une enquête sur une personne. Quand bien même vous la feriez faire et auriez des informations, vous ne pourriez pas en faire état.
Si vous, auditeur, avez identifié des indices de fraude, vous les faites remonter au directeur de l'audit. Le directeur de l'audit demande à l'auditeur ou à l'inspection de poursuivre. Si les indices deviennent de plus en plus pertinents, que la conviction devient quasi certitude, on passe alors au juridique. La question est : se sépare-t-on du fraudeur ou porte-t-on plainte ? Dans le deuxième cas, les services de police et les magistrats poursuivront l'opération.

© IFACI

Témoignage : Les contrôles transversaux dans les administrations

Noël PONS

Nous allons maintenant donner la parole à Didier DUVAL, pour l'exposé suivant. Didier DUVAL est contrôleur général, chef du pôle de lutte contre la délinquance financière, à la direction centrale de la police judiciaire au ministère de l'Intérieur.

Didier DUVAL, ***Contrôleur Général, Chef du Pôle de Lutte contre la Délinquance Financière, Direction Centrale de la Police Judiciaire, Minitère de l'Intérieur***

Je crois faire partie d'une génération, parmi les responsables de police, qui est dans une culture de très grande ouverture à l'égard d'un partenariat privé, ce qui me semble stratégiquement – et je n'ai pas peur d'utiliser le mot « stratégique » au sens plein et entier du terme – quelque chose d'indispensable aujourd'hui, compte tenu de la complexité des maux dont la société a à souffrir.

Les fraudes, au sens large, sont un vieux fonds de commerce de la police judiciaire. Ce que l'on appelle fraudes au sens générique, c'est ce que nous appelons, nous, la délinquance astucieuse, étant considéré que l'on part d'un postulat qui est que toute fraude n'a pas pour finalité un champ pénal, mais que toute infraction pénale, en matière économique et financière, a pour origine une fraude. Vous comprenez donc l'intérêt que je peux avoir à la lutte contre les fraudes.

Il y a deux cultures pour approcher la lutte contre les fraudes, il y a une culture vue de la police judiciaire, que j'appellerai une culture passive, qui consiste, en gros, à attendre une information, ou à attendre une saisine de la part d'une autorité judiciaire, soit le procureur de la République, soit un juge d'instruction ; et on traite l'affaire. Et il y a une approche beaucoup plus proactive – et vous avez compris, à travers mon premier propos, que j'appartiens à cette deuxième école – qui consiste à ne pas attendre que l'on nous apporte une saisine, mais, au-delà de l'aspect purement répressif, à avoir une vision que j'appellerai d'intelligence presque économique sur la problématique, avec différents partenaires, publics ou privés, de l'approche de lutte contre les fraudes ; et éviter ainsi ce qui, je crois, est un mal français, à savoir le cloisonnement de nos structures, qu'elles soient publiques ou privées.
Le cloisonnement public, il est réel ; il est encore plus réel entre les acteurs publics et les acteurs privés ; et tout cela n'est pas bon. L'exemple anglo-saxon est, à mon avis, une parfaite démonstration de ce décloisonnement. J'ouvre une parenthèse : j'ai toujours été surpris, dans mes jeunes années de commissaire de police, de voir, à l'occasion de réunions internationales, la composition des délégations étrangères. Nous venions, nous, en tant qu'acteurs purement publics, c'est-à-dire la police, la gendarmerie et éventuellement les services fiscaux dans le cadre de la lutte contre la délinquance financière, tandis que les délégations britanniques, américaines, venaient avec un responsable de police, un grand chef d'entreprise... La richesse de leurs propos, de leur approche était beaucoup plus étendue et variée de par cette structure pluridisciplinaire.
Il faudrait donc instaurer, tout en respectant le cadre spécifique de chacun naturellement, ce que j'appellerai le partenariat, mais le partenariat qui permet notamment, par un jeu de mutualisation, de mettre en place des politiques d'alerte. C'est extrêmement important : partenariat = mutualisation = décloisonnement = synergie positive, laquelle synergie inciterait des partenaires privés – et je vais donner un certain nombre d'exemples concrets – à nous faire part de leurs découvertes. Cette nouvelle conception permettrait une meilleure réactivité dans deux domaines : celui de la formation de nos collaborateurs, parce qu'on entrerait ces modes opératoires nouveaux dans un cursus de formation, ce qui veut dire une prédisposition intellectuelle et professionnelle à performer la lutte contre ce type de fraude ; et celui d'une coopération policière et judiciaire accentuée.

© IFACI

Le meilleur axe de coopération, ce n'est pas, là encore, d'attendre passivement que nos collègues étrangers, de quelque endroit du monde, nous avisent d'une malversation avec des retours en termes de sécurité intérieure, c'est celui d'avoir une politique de proactivité ; et comment pratique-t-on une politique de proactivité ? En créant comme on l'a fait il y a une quinzaine d'années, les attachés de sécurité intérieure. La France, aujourd'hui, fait partie des pays européens qui ont le plus d'attachés de sécurité intérieure dans les différentes ambassades françaises à l'étranger, puisque nous avons aujourd'hui cent douze ASI, plus les officiers de liaison, ce qui veut dire que trois cent cinquante officiers de police de tous grades (y compris nos collègues de la gendarmerie) occupent le terrain international ; et je peux vous dire que c'est une grande richesse pour assurer la mission première de la police judiciaire qui est de lutter contre le crime organisé.

Les affaires judiciaires traitées par la police judiciaire en France ne représentent que 3,5 % des infractions mentionnées sur l'état 4001, ce qui est très peu. Ceci étant, c'est ce que l'on appelle les faits constatés. Si on les évalue en termes de préjudice, les choses sont totalement différentes puisque, par définition, travaillant sur le crime organisé, nous nous attaquons forcément à des personnes qui ont la capacité à la fois morale, intellectuelle et financière de faire très mal à une économie, et même à une démocratie.
La mondialisation de l'économie veut dire qu'il y a aujourd'hui une grande facilité, pour les acteurs de la délinquance astucieuse qui sont sur le terrain de la fraude, de pouvoir se glisser à travers les mailles du filet. En conséquence – et je donnerai tout à l'heure un exemple très concret dans le domaine de la fraude sociale –, ce que l'on aurait pu appeler, il y a une dizaine d'années, « la fraude à papa », est devenu aujourd'hui quelque chose de très structuré qui alimente les revenus et les objectifs du crime organisé.
Le crime organisé travaille en fait sur un concept et un précepte très simples : analyse du risque pénal minimum et perspective de profit maximum. Lorsque cette équation se réalise dans un champ national, vous êtes sûr que les organisations criminelles vont s'engouffrer dans ce champ national.

Dans mon propos introductif j'ai voulu insister sur le décloisonnement qui est une notion essentielle en matière de lutte contre la fraude, décloisonnement entre acteurs publics, et entre acteurs publics et privés. Concernant le premier, je citerai l'effet GIR, les groupes d'intervention régionaux, voulus, mis en place et impulsés par M. Sarkozy en 2002, lorsqu'il était ministre de l'Intérieur. Pourquoi parle-t-on d'effet GIR ? Parce que la mise en place de ces groupes a effectivement permis, institutionnellement, de décloisonner différents partenaires publics, en l'occurrence la police, la gendarmerie, les impôts, la douane, la DGCCRF, et un peu en satellite, l'Inspection du travail. Ce qui est extrêmement important c'est que, dans cette approche de lutte contre la fraude, c'est l'échange d'informations, mais aussi l'approche pluridisciplinaire au plan technique de chacune de ces composantes qui apporte la richesse et une capacité de riposte à la lutte contre la fraude ; pour les GIR, en deux mots, axée essentiellement sur la délinquance dite de proximité et de ce que l'on appelle plus particulièrement l'économie souterraine dans les zones urbaines sensibles, avec d'ailleurs toute une législation que j'évoquerai tout à l'heure, qui a beaucoup évolué sur la notion de non justification de ressources. On introduit donc, en droit pénal, dès 1996, dans le contexte de la lutte contre le trafic de stupéfiants, cette notion de non justification de ressources, qui est aujourd'hui un outil extrêmement intéressant pour aller au-delà du dispositif anti-blanchiment datant de 1990. La notion de non justification de ressources nous donne les bases légales (loi du 23 janvier 2006), police et justice, de pouvoir interroger la personne sur l'origine légale ou non des fonds qui lui ont permis d'acquérir ses biens ; et si la réponse ne satisfait pas l'autorité judiciaire, le suspect passe, comme on dit, en voie de condamnation et c'est là que se referme la boîte de l'illégalité et de l'immoralité de s'enrichir à partir de la commission d'infractions illégales.

Un autre aspect de ce décloisonnement entre partenaires publics et privés, beaucoup plus récent, est le blanchiment qui, à partir des années 1990, a impulsé considérablement ce partenariat, certes au départ difficile culturellement, notamment pour le monde de la banque et le monde de l'assurance, mais qui aujourd'hui apporte, même si ce n'est pas une panacée, une plus-value considérable.

Un exemple de décloisonnement d'acteurs publics : la lutte contre le faux monnayage. L'office central du faux monnayage, créé en 1929 – c'est le premier office qui a été créé dans le cadre de la Convention de Genève en

 © IFACI

matière de lutte contre le faux monnayage –peut travailler en décloisonnement des services répressifs, notamment police et gendarmerie, et travailler aussi avec d'autres partenaires que les institutions dites de sécurité intérieure, en l'occurrence la Banque de France et, depuis le passage à l'euro en 2002, avec la Banque centrale européenne. Tout cela impulse une grande synergie, en permettant notamment à la Banque de France et à la Banque centrale européenne de donner aux offices centraux des différents pays de la zone euro des clés d'analyse sur les lieux d'émission, étant considéré que, sur l'ensemble des faux billets répertoriés, 85 % de ces billets sont répertoriés par la Banque de France et, par là même, par le secteur bancaire.
Les faux moyens de paiement, outre la fausse monnaie papier, la fausse monnaie métallique, les faux chèques, ce sont aussi les cartes bancaires : c'est aujourd'hui une forme de fraude qui explose et qui est directement liée à des phénomènes de mondialisation de l'économie.

Avec la fraude par carte bancaire, on est dans le domaine du numérique, c'est pourquoi il a été décidé, à la police judiciaire, d'exporter une brigade spécialisée de lutte contre les cartes bancaires de l'Office central du faux monnayage, à un nouvel office créé le 15 mai 2000, qui est l'Office central de lutte contre la criminalité liée à la technologie de l'information et des communications, ce que l'on appelle plus concrètement la cybercriminalité ; fondamentalement, le support d'une fausse carte, c'est aujourd'hui un support numérique, soit dans la piste, soit éventuellement dans la puce. Aujourd'hui, nous sommes confrontés à des problèmes de mondialisation. Nous avons identifié un individu qui a, par voie numérique, capté environ 150 000 références de cartes bancaires sur le continent nord-américain. Cette personne est en train actuellement de reproduire et de dupliquer, à partir de ces références de cartes bancaires, des fausses cartes qu'on appelle des *white cards*, et qu'il va mettre sur le marché très prochainement, au prix de 50 dollars la carte. Faites le calcul ! Evidemment nous ne le laisserons pas réaliser son rêve, et ce grâce à un travail de partenariat avec l'équivalent américain du GIE Carte bancaire et des acteurs de lutte contre la cybercriminalité américaine.

Dans le secteur de la cybercriminalité, l'Office des nouvelles technologies travaille sur tous types de fraudes, et notamment sur certains modes opératoires comme le *phishing*, le *skimming*, en particulier sur les distributeurs automatiques de billets, bref, toutes actions qui sont fortement préjudiciables, non seulement à ceux qui interrogent à distance leur banque, ou qui retirent des billets dans un DAB, mais en raison des manipulations, des duplications de ces références bancaires, à une échelle considérable.
Dans le secteur de la cybercriminalité qui est extrêmement large, il a été constaté des fraudes dans un domaine très sensible qui est le commerce électronique. Dans ce domaine il y a une explosion en termes de chiffre d'affaires potentiel, donc en termes de stratégie économique du commerce électronique. Si nous ne réagissons pas rapidement et fermement pour fiabiliser ces opérations, ce sont des pans entiers de développement économique qui s'effondrent. Il est donc vital que les relations que nous avons aujourd'hui avec les opérateurs ou les fournisseurs d'accès Internet, nous permettent cette proactivité opérationnelle, donc judiciaire, extrêmement prégnante.

J'ai évoqué tout à l'heure la lutte contre le blanchiment et le financement terroriste, comme référence du décloisonnement d'acteurs publics et d'acteurs privés. En 1989 est créé le GAFI, organe de lutte contre le blanchiment à l'échelle planétaire. A partir de là, chaque pays adhérent au GAFI crée ses propres structures : en France, c'est TRACFIN, qui recense l'ensemble des déclarations de soupçon des professionnels assujettis à l'obligation de déclaration de soupçon ; et c'est, au plan répressif, l'Office central de répression de la grande délinquance financière (OCRGDF) avec ses partenaires naturels au plan territorial pour la police judiciaire que sont les divisions économiques et financières. Tout cela crée un grand maillage, du côté administratif géré par le ministère des Finances (TRACFIN), et du côté de la police judiciaire (l'OCRGDF). Pour moi, la grande avancée de ce dispositif, ce n'est pas seulement la création de TRACFIN et de l'OCRGDF, ce n'est pas seulement la création de bases légales – les articles 324-1 et suivants du code pénal en matière de lutte contre le blanchiment – c'est l'implication de tout un pan du secteur privé amené à gérer de près ou de loin des fonds dans une dimension partenariale de sécurité.
Le dispositif anti-blanchiment TRACFIN nous permet aujourd'hui de recenser annuellement environ 12 000 déclarations de soupçon. Sur ces 12 000 déclarations, TRACFIN en transmet 400 à la Justice, au procureur de

la République. Très peu de ces déclarations font l'objet d'un classement sans suite ; la quasi totalité est reversée aux services de police, notamment à l'Office central ou aux divisions financières, en vue d'un traitement judiciaire. Actuellement, nous avons entre 350 et 400 affaires en cours sur le territoire national, ce qui veut dire que nous faisons prendre conscience au crime organisé que, lorsqu'il vient investir en France, il arrive dans un environnement de risque pénal, ce qui, pour lui, n'est pas neutre. Tout cela est rendu possible grâce au partenariat public/privé, sans lequel notre capacité de riposte serait absolument dérisoire.

La fraude sociale.
Un protocole a été signé le 26 janvier 2007 entre le directeur général de la police nationale, le directeur général de la gendarmerie et le président de la CNAM. Ce protocole décrétait la mise en place, au sein de la CNAM et des 128 caisses primaires d'assurance maladie, d'un dispositif de lutte contre les fraudes, grâce à une réactivité humaine par la connaissance des mécanismes de la fraude, et à la mise en place d'outils informatiques permettant de créer des alertes dès lors qu'un processus anormal intervenait dans le paiement de certaines prestations d'assurance maladie. En outre, nous avons, dans ce protocole, prévu et orchestré les correspondants, c'est-à-dire que nous avons supprimé ce temps de latence de réactivité entre les différents partenaires : si une caisse primaire d'assurance maladie détecte une fraude et que, en interne, elle décide de franchir le Rubicon et de la traiter au plan judiciaire, le protocole prévoit quel est le correspondant à contacter immédiatement. Cela a, pour nous, un intérêt considérable qui est que pour les fraudes de cette nature – mais que l'on peut étendre à d'autres types de fraude sociale, et nous sommes d'ailleurs actuellement en train de préparer un protocole dans le même esprit avec l'UNEDIC en matière de prestations liées à l'assurance chômage – cela nous permet, à nous, au plan judiciaire, de travailler au temps de la commission d'infraction. Autrement dit, le fonctionnaire va pouvoir travailler dans un temps où il aura une grande chance de pouvoir interpeller non seulement les comparses, les porteurs de valise qui, dans le contexte du crime organisé, travaillent pour le compte d'un auteur intellectuel (lequel retirera tous les profits financiers de l'affaire et ne prendra aucun risque pénal), mais aussi ce dernier. Travailler au temps de la commission d'infraction, c'est pouvoir utiliser toute notre logistique judiciaire : les surveillances, les écoutes, etc., afin d'être efficace dans un contexte de crime organisé. Autre avantage, cela nous permet, à nous aussi, une très grande réactivité en termes de traçabilité des flux qui sont illégalement arrivés dans la poche des délinquants. On ne travaille plus six mois, huit mois, douze mois après les faits, c'est à dire sur de la matière morte.
Voilà quelques-uns des aspects très positifs du travail en partenariat dans la lutte contre les fraudes.

Les problématiques de traitement des fraudes dans les filiales étrangères

Noël PONS

Nous allons poursuivre avec Dmitri KOSSAREV qui va nous parler des problématiques de traitement des fraudes dans les filiales étrangères. Dmitri KOSSAREV est directeur du département Litiges et Investigations chez PricewaterhouseCoopers.

Dmitri KOSSAREV, ***Directeur du Département Litiges et Investigations, PricewaterhouseCoopers***

Nous allons donc analyser la problématique de la fraude dans les filiales, notamment les filiales étrangères, et essayer d'enrichir cette analyse avec quelques exemples, quelques idées, quelques réflexions.
Rappelons ce qu'est la fraude en nous référant au triangle de la fraude. Le triangle de la fraude est aussi appelé parfois triangle de Cressey. Donald Cressey est un Américain qui a fait des recherches sur la fraude, et sur le

 © IFACI

comportement des individus. Il a eu des entretiens avec environ deux cents criminels emprisonnés aux Etats-Unis. Sur la base de ces discussions, il est arrivé à la conclusion suivante : 10 % d'individus ne frauderont jamais ; 10 % d'individus essaieront toujours de frauder ; 80 % d'individus ne sont pas prédisposés à frauder, mais ce sont les circonstances qui décideront. Le triangle a été conçu pour comprendre ce qui poussait des individus pas spécialement prédisposés à frauder, mais exposés à frauder, à le faire. Lorsq'une fraude est commise, trois conditions sont réunies, qui sont les trois angles du triangle : la motivation/pression ; l'opportunité ; la rationalisation/justification.

La motivation/pression.

Dans les filiales, ce sont les pressions et les motivations traditionnelles : une compensation significative, si le budget est respecté et dépassé. Je sais que les groupes, maintenant, font de gros efforts en matière de rémunération de dirigeants ou de responsables financiers des filiales à l'étranger, pour déconnecter au maximum la partie variable d'une simple approche et du calcul mathématique : « si le chiffre du budget est respecté, vous allez avoir tant ». Beaucoup de groupes ont décidé d'introduire des éléments beaucoup plus qualitatifs dans le calcul des bonus des responsables des filiales, ce qui est un grand progrès. Néanmoins, on trouve encore des cas où bonus et récompenses sont octroyés sur des bases plus mathématiques que qualitatives, ce qui présente un risque et crée une motivation.

On trouve aussi, dans les filiales, des situations un peu plus subtiles, par exemple, la possibilité du fonctionnement indépendant, avec le raisonnement : « pas de questions tant que le budget est fait ». Cela arrive souvent, dans les configurations où les filiales fonctionnent d'une manière indépendante. Par exemple, quand on intervient dans l'investigation des fraudes et que l'on essaie de comprendre les raisons, nous obtenons des réponses du type : « Oui, mais de toute façon, historiquement, du moment que ma marge opérationnelle ou marge brute ou résultat avant impôt était dans le budget, personne ne posait de questions. Ça allait très bien. »

On trouve des comportements, au plan local, qui consistent à aménager des packages de rémunération locaux, à pratiquer une indexation dans le contrôle des dépenses ; on commence par les notes de frais, mais au fur et à mesure, cela crée un effet boule de neige qui pousse vers des comportements beaucoup plus nuisibles.

Il y a des situations spécifiques, comme la situation des filiales récemment acquises et des dirigeants historiques restés aux commandes. Un exemple, parmi beaucoup d'autres : il y a quelques années, une entreprise a acquis une société familiale aux Etats-Unis. Cette société familiale, gérée d'une manière traditionnelle, est donc entrée dans un groupe extrêmement structuré, avec des objectifs précis, des indicateurs de performance, etc. Une très forte pression s'exerçait sur les dirigeants de la société familiale qui n'avaient jamais eu l'habitude de travailler dans un tel environnement. A un moment donné, comme l'environnement économique (il y avait une crise économique aux Etats-Unis) était mauvais, et la pression très forte, ils ont « dérapé » et manipulé les chiffres comptables pour présenter des résultats en décalage avec la réalité.

L'opportunité.

Les filiales étrangères ont **des spécificités environnementales.**

Les différences culturelles, tout le monde sait ce que c'est. Un groupe de chercheurs a essayé d'analyser les différences de perception du même sujet par les Occidentaux et les Asiatiques, notamment les Japonais. Ces chercheurs ont fait des groupes de travail composés exclusivement d'Occidentaux et exclusivement de Japonais, et ils ont présenté une photo en demandant: « Qu'est-ce qui vous attire dans cette photo ? Qu'est-ce qui vous saute aux yeux immédiatement ? Donnez-nous votre première impression. » Les Occidentaux étaient frappés par une impression d'ensemble ; les Japonais se concentraient sur les détails.

Si l'on transpose cet exemple au contrôle interne, on constate que la notion même du contrôle interne n'est pas appréciée de la même façon par les uns et les autres. Les réactions sont différentes. Un système de contrôle efficace en France n'est pas forcément approprié dans un autre pays, dans un environnement culturel différent. Des adaptations, des aménagements sont presque toujours nécessaires.

Les pratiques locales et les partenaires locaux sont aussi un sujet important. Quand on arrive dans un pays pour la première fois, on a recours à des agents pour nous aider à présenter des appels d'offres. Or, parmi ces agents, certains sont malhonnêtes et emploient des moyens illicites pour présenter l'offre, pour être assurés de toucher

la commission en cas de réussite. Il y a là un risque pour l'entreprise dont la responsabilité peut être mise en cause.

Autre sujet très important : ce que les Anglo-saxons appellent *tone at the top*, c'est à dire la culture de contrôle que l'on essaie de développer dans l'entreprise, et de transmettre aux filiales. Mais il arrive que l'essence de cette culture se perde en cours de route, surtout si elle est communiquée d'une manière inappropriée. Le message fort que l'on perçoit dans la maison mère n'aura pas alors le même impact au niveau local.

Enfin, un problème typique que tous les auditeurs rencontrent dans le cadre de leurs audits à l'étranger, est une familiarisation insuffisante avec les politiques et procédures du groupe et avec les lois et réglementations. S'il n'existe pas de supervision forte et constante, le respect de ces lois et règlements sera petit à petit perdu de vue ou contourné.

Les filiales étrangères ont **des spécificités structurelles.**
Les filiales étrangères sont souvent en butte à des problèmes d'organisation, lesquels débouchent à terme sur des lacunes de contrôle interne pouvant être exploitées par des fraudeurs. De même la responsabilité diluée en matière de contrôle interne et l'insuffisance des ressources dédiées au contrôle, peuvent être à l'origine de fraudes.
Lorsque la croissance opérationnelle dépasse les ressources des fonctions de support, lorsque le business prend le dessus, il y a également un risque fort.
Autre risque, celui des lignes de *reporting* inadaptées : il n'y a pas longtemps, dans beaucoup d'entreprises, le contrôleur financier local rapportait au dirigeant opérationnel de l'entité ou de la zone géographique où l'entité opérait. Le système a changé, et maintenant les contrôleurs financiers des filiales rapportent aux contrôleurs financiers des zones et du groupe.
Les systèmes informatiques hétérogènes : les filiales – notamment les filiales éloignées – ne disposent pas toujours des mêmes systèmes d'information que le siège, et les projets informatiques sont rarement prioritaires dans les filiales, ce qui crée des problèmes, notamment pour le *reporting* groupe, quand il faut utiliser un système différent. Il s'ensuit des saisies manuelles, des ajustements, toutes opérations propices à la manipulation des chiffres.
L'absence sur place de managers suffisamment expérimentés crée une fragilité dans les petites filiales.

La rationalisation/justification.
C'est un sujet psychologique. A mon avis, ce type de comportement est lié aux spécificités culturelles. On entend souvent des raisonnements du type : « crimes sans victime, ce n'est rien pour une multinationale, compte tenu des profits réalisés sur place et dans le monde ».
Dans un cadre d'économies d'échelle et de restructurations, le risque important est que des individus soient déçus et que cette déception se traduise par des actes inappropriés.
Les coutumes locales : « tout le monde fait comme cela, ici ». Les personnes qui travaillent pour une grande organisation structurée ne comprennent pas pourquoi elles devraient se comporter différemment que dans une petite entreprise locale où il y a parfois confusion entre patrimoine personnel et patrimoine de l'entreprise.
Les possibilités de collusions internes et externes sont assez fréquentes : on fait travailler la famille ; les fournisseurs font partie de la famille ou sont des connaissances. Tout cela crée des situations qui ne sont pas saines, où la séparation des tâches n'existe pratiquement plus.

Après ce tableau un peu sombre nous allons voir quels sont les moyens à mettre en place pour faire bien fonctionner une filiale, et pour prévenir la fraude.

Le traitement des fraudes.
En matière de **prévention** ce qui est primordial, c'est une communication effective des valeurs éthiques du groupe. C'est indispensable, car souvent on se rend compte que des personnes ayant commis une fraude, ne comprennent même pas la portée de leur acte. C'est pourquoi il faut insister sur les valeurs du groupe, la

 © IFACI

culture de contrôle, etc.
La sensibilisation et la formation du personnel sont aussi très importantes pour la prévention de la fraude, notamment auprès des personnels chargés de cette prévention (les contrôleurs) auxquels il faut bien expliquer les risques et les enjeux.
Ethics hotline, whistleblowing ou alerte professionnelle sont les trois noms souvent utilisés pour tous les systèmes de reporting des actes illégaux commis dans les entreprises. C'est un concept né dans les entreprises américaines, et qui est maintenant appliqué par plusieurs groupes en Europe, notamment ceux qui sont cotés aux Etats-Unis. Est-ce une mesure de prévention ? Oui. Beaucoup pensent que c'est un outil de dénonciation qui va faire remonter tous les coups tordus montés dans les filiales éloignées. Ce n'est pas mon opinion : je ne perçois pas cet outil comme un outil de remontée des indices de fraude, mais je pense que la vraie valeur ajoutée de cet outil, c'est la dissuasion. Les personnes qui savent qu'il existe un outil de *reporting* des alertes, vont peut-être réfléchir à deux fois avant de commettre un acte illégal. C'est dans tous les cas un outil qu'il faut manier très précautionneusement.

La procédure d'embauche aux postes sensibles est aussi un sujet délicat. Je connais le cas d'un trader qui s'était livré à une malversation dans l'établissement financier qui l'employait, malversation exactement identique à celle qu'il avait réalisée dans un établissement précédent. Si une enquête avait été effectuée avant son recrutement, la fraude n'aurait pas eu lieu.
Une investigation effective et immédiate des indices de fraude : il y a beaucoup d'enjeux dans cette réaction. Une réaction rapide donne beaucoup plus de possibilités de récupérer les actifs, si c'est un détournement d'actifs, et donne aussi les moyens de ne pas communiquer d'informations erronées dans les états financiers, de mettre en place les actions correctives très rapidement.

La communication est particulièrement utile. Une bonne communication sur une fraude survenue dans une filiale, montre que le groupe prend en charge les situations difficiles, que les événements sont gérés rapidement, et surtout qu'une fraude ne reste pas impunie. Pour l'environnement de contrôle, c'est un très bon message qui doit être diffusé aux employés, surtout dans les zones sensibles.

On peut mettre en place des mesures de prévention structurantes comme le rattachement hiérarchique des contrôleurs locaux aux responsables du contrôle du groupe, plutôt qu'aux dirigeants opérationnels locaux. C'est une mesure de bon sens qui permet d'éviter beaucoup de cas de fraude.

On peut mettre en place aussi des missions périodiques d'audit interne : il est absolument indispensable, à mon avis, de s'assurer que les missions d'audit couvrent, sur une base pluriannuelle et d'une manière exhaustive, tout le périmètre du groupe. Je sais que les équipes d'audit interne ne sont pas toujours très étoffées, notamment dans les groupes où il y a beaucoup de croissance, beaucoup d'activités. C'est pour cela que certains groupes cherchent des solutions, comme de faire des missions d'audit interne conjointement avec les consultants externes ou d'étoffer les équipes internes en créant des relais au niveau local.
Quoi qu'il en soit il faut que les filiales soient auditées une fois tous les deux ou trois ans, pour s'assurer de la performance des systèmes de contrôle interne et ne pas laisser se créer un climat et un environnement susceptibles de favoriser la fraude.

Il ne doit pas exister de zones « restreintes » : on a vu récemment des cas où des fraudes significatives se sont produites dans des filiales qui étaient « interdites », pour diverses raisons, aux équipes de l'audit interne. Si, dans un groupe, certaines entités opposent une résistance à la venue d'équipes d'audit interne, c'est, à mon avis, un signal d'alerte à prendre en compte immédiatement.

En matière de **détection** des fraudes, la remontée des alertes par les canaux internes et externes, est assez courante. Même si les alertes externes sont plus rares, et ne méritent pas toujours d'être prises au sérieux, il ne serait pas non plus prudent de les rejeter systématiquement.

© IFACI

La communication avec les auditeurs externes est toujours intéressante et souvent enrichissante. Leur cadre professionnel, leur cadre de travail est différent de celui des auditeurs internes ; les seuils de matérialité, les seuils de reporting diffèrent aussi de ceux du groupe, et peuvent faire apparaître des dysfonctionnements ou des anomalies qui sont des sources d'informations à prendre en compte.

L'intégration systématique du volet risque de fraude dans les missions périodiques de l'audit interne est indispensable. Le volet risque de fraude, s'il est traité en collaboration avec l'audit externe, peut avoir une réelle valeur ajoutée.

Concernant **l'investigation**, je dirai deux choses. Premièrement : intervenir le plus vite possible suite aux signaux d'alerte. Plus on intervient tôt, plus on a de chances de récupérer les actifs, d'arrêter la fraude, d'éviter des pertes, et de communiquer des informations financières exactes. Deuxièmement, rassembler les ressources et les compétences nécessaires (internes et si nécessaire externes) : compétences opérationnelles pour comprendre les produits et leur fonctionnement ; connaissance des spécificités locales (langue, culture, habitudes, moyens d'investigation informatiques) ; compétences réglementaires (fiscalité, gestion sociale).

En conclusion, le rôle de l'audit est de concevoir ou de veiller à la conception de bons moyens de détection et de prévention de la fraude dans l'entreprise. Le positionnement d'une filiale à des milliers de kilomètres du siège, dans un pays étranger, ne doit pas la faire « bénéficier » d'un régime fondamentalement différent de celui du siège. Le niveau de contrôle doit être le même, la fréquence des missions également. Il appartient à l'audit interne de veiller à ce qu'il en soit ainsi.

Noël PONS

Merci, M. KOSSAREV, pour la clarté de votre exposé. Y a-t-il des questions sur ce problème qui est sans doute le problème le plus important, actuellement. De par la mondialisation des opérations, le *reporting* des filiales n'est pas neutre.

QUESTIONS

Question

Concernant les sources de fraude, aujourd'hui on entend parler d'une part, de petites pertes récurrentes provenant de détournements ou de failles informatiques que certains collaborateurs savent utiliser ; d'autre part, on entend pas mal parler de systèmes de rémunération, et de systèmes beaucoup plus organisés.
Quel est votre sentiment ? Les groupes sont-ils aujourd'hui plutôt confrontés aux uns ou aux autres ?

Dmitri KOSSAREV

C'est une très bonne question, mais très difficile.
Je pense que les groupes sont confrontés à deux problèmes en même temps. La criminalité organisée bénéficie de moyens financiers et techniques extrêmement importants, et elle évolue en permanence. Elle utilise des moyens technologiques de plus en plus sophistiqués, et est parfois très en avance sur les entreprises dans le domaine technologique comme en compétences. Le risque vient de là.
En ce qui concerne les petits vols des employés qui utilisent les petites failles informatiques oui, l'informatique est un domaine qui progresse énormément, qui évolue sans cesse, et des failles apparaissent tout le temps. Oui, les deux types de fraude existent, mais les enjeux et les moyens de promotion sont sans doute différents.

Noël PONS

Je voudrais vous poser une question, M. KOSSAREV, concernant le directeur financier et le contrôleur finan-

© IFACI

cier, dans une filiale. Y a-t-il une problématique spécifique à l'égard des fraudes ? En clair, est-ce que ce sont des postes à risque ?

Dmitri KOSSAREV

Je pense que, dans une filiale, le risque du poste de directeur financier ou de contrôleur financier est lié à la petite taille des entités. Le contrôleur financier ne bénéficie pas de la même séparation de fonctions qui existe, par exemple, dans la maison mère ou dans une grande filiale. Et quand il n'y a pas de séparation des tâches, il y a de fait beaucoup plus d'opportunités. C'est dans ce sens que le poste de contrôleur financier, à mon avis, est à risque. C'est un poste à risque, parce qu'il expose la personne : opportunités, pressions inutiles... Même si la personne est tout à fait intègre au début, elle est placée dans une situation difficile.
C'est pour cela que, quand une fraude est due à un dysfonctionnement dans le *reporting* ou la séparation de tâches, on ne peut pas dire que c'est la faute de la personne. C'est une erreur du dispositif, et c'est une erreur du groupe qui n'a pas bien analysé le problème, mettant ainsi l'individu dans une situation inconfortable, voire dangereuse.

L'entreprise, cible des fraudeurs : comment l'audit interne peut-il la protéger ?

Noël PONS

Nous allons poursuivre et terminer la journée avec une table ronde, à laquelle participeront Xavier BREGOU, directeur de l'audit interne du groupe PPR ; Marc CHAMBAULT, gérant associé de France MC conseil ; Jean-Yves PELISSON, directeur de l'audit général groupe AGF.

Marc CHAMBAULT, *Gérant-Associé, France MC Conseil*

Je reviens du Canada, avec un certain nombre de membres de l'IFACI, où nous avons assisté à plusieurs conférences, dans le cadre du chapitre canadien de l'IIA. J'ai constaté – c'est un témoignage que je peux apporter – combien, dans les pays nord-américains, le traitement de l'information sur les fraudes s'est perfectionné. En trois ans, j'ai vu un changement de panorama impressionnant.

Est-ce l'effet Sarbanes-Oxley ? Très certainement, au moins en partie. Est-ce la prise de conscience des entreprises, l'importance économique de la fraude ? Mais j'ai vu – et cela m'a particulièrement frappé – un panorama statistique complètement modifié : des présentations où l'on sait tout sur le fraudeur, son âge, le *modus operandi*, la sociologie, s'il fraude seul ou non, l'impact financier de chaque fraude, la typologie des fraudes elles-mêmes, qu'elles soient financières ou autres. Bref, une base de données statistique constituée à partir d'un certain nombre d'études extrêmement approfondies.

J'ai retenu un chiffre : les entreprises américaines considèrent, d'après ces sondages et statistiques, que la fraude leur coûte 5 % du chiffre d'affaires. 5 % du chiffre d'affaires, c'est plusieurs centaines de milliards de dollars qui disparaissent chaque année dans le cadre de ces opérations de fraude. C'est donc un enjeu économique considérable. Ma deuxième remarque, c'est qu'il n'y a pas d'entreprises qui représentent le modèle type de la moyenne de ces statistiques. Chaque entreprise a ses propres spécificités. Chaque entreprise doit réfléchir sur ses structures de risque en matière de fraude. Je pense d'ailleurs que l'approche des structures de risque en matière de fraude est assez voisine, voire équivalente aux approches classiques en matière de risque.

© IFACI

Une fraude survient quand il y a une probabilité que la fraude existe. On voit, au travers des études nord-américaines, qu'en fait la probabilité s'effondre quand des dispositifs de contrôle (contrôle interne permanent, contrôle périodique de l'audit interne) sont mis en place.

Quand une fraude se produit, il y a un risque financier. Il peut aussi y avoir un risque d'image, et les dirigeants peuvent être impliqués dans des affaires juridiques complexes. On voit donc que tous les ingrédients pour un traitement du type cartographie des risques sont réunis et de plus en plus de sociétés sont engagées sur la voie de la cartographie, parce qu'aucune société ne ressemble à une autre. Chaque société a ses risques. Il est certain, par exemple, que les risques de France Télécom qui est implantée dans cent cinquante pays et qui a cent cinquante millions de clients, sont différents de ceux d'une PME qui n'a pas d'activité à l'international.
Chaque entreprise doit donc analyser ses risques et faire apparaître ses risques majeurs de façon – et on en parlera probablement tout à l'heure – que les processus clés en face de ces risques majeurs soient parfaitement identifiés, afin que le contrôle interne puisse intervenir, de manière ciblée, sur les points les plus critiques.

Une dernière remarque : la terminologie est parfois confuse. Chez France Télécom, la fraude externe, c'est du vol : un client qui trafique sans payer, vole l'entreprise ; on peut voler du trafic, on peut voler des terminaux. Ce sont des opérations de vol regroupées sous la dénomination de fraude externe.

La fraude interne est liée à des comportements non éthiques. On peut retrouver, dans des groupes, des risques potentiels de fraude liés par exemple à la décentralisation (décentralisation sur les achats) ; si les filiales sont nombreuses, il y a évidemment des risques de conflit d'intérêt ou des risques financiers, quand elles font des opérations d'encaissement et de décaissement, surtout dans des pays éloignés.
Chaque entreprise doit donc, en fonction de ses risques – ses risques pays, ses risques structurels, ses risques d'activité – analyser ses priorités.

Noël PONS

Je vais donner la parole à M. BREGOU sur trois thèmes : d'abord la notion de fraude dans le secteur d'activité. Ensuite, les dispositifs de prévention et de traitement dans ce type d'entreprise. Enfin, le positionnement de l'audit interne pour protéger l'entreprise.

Xavier BREGOU, *Directeur de l'Audit Interne du Groupe, PPR*

Le Groupe PPR a deux activités : la distribution et le luxe.

Je vais vous citer quelques unes de nos enseignes, et vous comprendrez mieux les difficultés que nous rencontrons avec la problématique de la fraude : la FNAC, CONFORAMA, je pense que vous connaissez. CFAO, dont l'activité essentielle est de distribuer des véhicules automobiles et des médicaments en Afrique ; on touche là un autre continent, et un autre type d'activité. LA REDOUTE, activité de vente à distance : autre problématique. Dernière enseigne, qui touche le luxe, GUCCI Group, qui traite l'ensemble des marques GUCCI et Yves Saint-Laurent.
Contrairement à ce que vous expliquait M. CHAMBAULT, pour nous, la notion de vol, c'est la notion de fraude. Le vol est un type de fraude, laquelle existe dans l'ensemble de nos magasins. Cela dit, il y a aussi la fraude comptable, la fraude financière, etc. Un autre type de fraude sévit dans notre activité de luxe qui est la contrefaçon
Comme il a été dit, il faut recenser l'ensemble des risques susceptibles de générer de la fraude, et les hiérarchiser.
Dans le groupe PPR, on traite en même temps la fraude interne et la fraude externe, parce que l'on considère que, parmi les voleurs, un tiers viennent de l'extérieur, un tiers font partie du personnel, et un tiers viennent d'on ne sait où, mais existent bel et bien. Il nous faut donc lutter à la fois en interne et en externe.
Nous accentuons énormément nos travaux sur le contrôle interne, le but du jeu étant de sécuriser l'ensemble

 © IFACI

des flux et l'ensemble des chaînes économiques et logistiques, d'agir préventivement, notamment dans le domaine de la contrefaçon, fléau mondial.

Jean-Yves PELISSON, *Directeur de l'Audit Général Groupe, AGF*

J'aimerais réagir après les présentations de mes deux collègues.
Sur les problèmes évoqués par M. CHAMBAULT, j'ai un point d'accord et un point de désaccord.

Le point d'accord, c'est qu'il n'existe pas d'organisation standard de lutte contre la fraude. Si je prends le cas de mon groupe – Allianz et ses filiales, dont AGF – nous n'avons pas de politique générale contraignante nous obligeant à mettre en œuvre telle ou telle disposition d'organisation dans nos structures, alors que c'est le cas pour l'audit.
La fonction audit répond à des politiques extrêmement précises qui nous imposent d'être organisés d'une certaine façon, avec des lignes de *reporting*, avec des méthodes. Dans le cas de la fraude, ce n'est pas le cas. Nous avons simplement des lignes directrices qui donnent des recommandations générales autour desquelles nous pouvons nous organiser, l'organisation de chacune des entités dépendant d'une analyse des risques de fraude, des activités, de la culture de l'entreprise. Je reviens sur ce que l'on évoquait il y a quelques minutes sur les filiales étrangères : l'organisation du dispositif de lutte contre la fraude ne sera pas la même dans notre filiale brésilienne et dans notre filiale libanaise. L'organisation de la fraude doit être adaptée aux spécificités de chaque entité.

Le point de désaccord porte sur la question de la définition de la fraude. Il me semble très important, à partir du moment où on veut lutter contre la fraude, de donner une définition, dans chaque organisation, globalement conforme aux principales références qui existent en la matière. Dans le cas d'un groupe comme Allianz où nous sommes sous les fourches caudines de SOX, il est assez facile de se référer à des définitions de la fraude existantes, encore faut-il que ces définitions soient comprises et partagées par le management de l'entreprise.
Au début de l'année 2006 nous avons rédigé une définition de la fraude, nous l'avons inscrite dans un projet de charte dédiée à la lutte contre la fraude, et nous l'avons présentée au comité exécutif de l'entreprise, pour validation. Je peux vous dire que ce n'est pas un exercice facile : trouver la formulation adaptée au contexte, expliquer les termes retenus, … En effet, dans un groupe comme AGF, nous sommes confrontés, en plus des fraudes classiques que l'on trouve dans toute organisation, à deux types de fraudes spécifiques. D'une part, dans le cadre de notre activité d'assurance dommages, aux fraudes classiques à l'assurance : les sinistres qui interviennent de façon exagérément opportune après le renouvellement des polices d'assurance, avec des couvertures majorées ; c'est ce que l'on appelle les fraudes externes, dont le préjudice potentiel est directement subi par l'entreprise. D'autre part, dans le cadre de notre activité de collecte de placements financiers, à un type de risque (que l'on trouve également dans le monde bancaire) associé à l'existence de réseaux de distributeurs qui, dans notre cas, représentent plusieurs milliers de personnes, et qui peut générer, par le biais d'une fraude le plus souvent interne, commise soit par un salarié, soit par un mandataire, au détriment du client, un préjudice financier pour l'entreprise ainsi qu'un préjudice d'image.

Ces deux spécificités sont la marque d'une compagnie d'assurance comme la nôtre, et c'est à partir de leur analyse que nous avons construit notre organisation de lutte contre la fraude.

Marc CHAMBAULT

Je suis absolument d'accord sur ce qui a été dit. Peut-être mes propos sur la définition de la fraude étaient-ils imprécis. Je voulais simplement insister sur le fait que c'est un exercice difficile, mais nécessaire. Je voulais surtout attirer l'attention sur un point : quand des statistiques sont émises dans le domaine de la fraude, il faut faire très attention sur les assiettes de définition utilisées, pour ne pas en tirer des conclusions hasardeuses.
Je crois que, pour prévenir et traiter la fraude, chaque société doit créer un environnement favorable au traitement de cette fraude. Cela se fait en plusieurs étapes.

© IFACI

Il faut d'abord un code éthique. L'éthique fait partie de la culture de l'entreprise. C'est d'ailleurs une des responsabilités de la *corporate governance* que de définir les grands principes, et de fixer les axes et les politiques sectorielles et opérationnelles, clairs. Les sociétés américaines qui ont mis en place un code éthique, ont divisé par deux l'impact financier des fraudes.
Il faut ensuite mettre en place des systèmes de contrôle permanent sur les processus à risque : effectuer des sondages, traiter les indices et les signes d'irrégularité rapidement, dès qu'ils se manifestent dans le suivi d'information.

Une fraude, une fois qu'elle est déclarée, doit être traitée. Les sociétés sont très diversement organisées sur ce point. On peut observer qu'il y a des entreprises (dans le monde bancaire, dans les sociétés de service, etc.) où les services d'enquête font partie de l'audit interne : le contrôle général, comme on l'appelle à France Télécom, ou l'inspection générale, dans les banques, sont dans le même ensemble que l'audit interne. Les structures sont un peu différentes dans les sociétés industrielles, ou dans les sociétés de distribution, qui sont très décentralisées, où on laisse au management local (management des usines ou des grandes surfaces), la responsabilité du traitement des affaires. Il existe d'autres configurations comme celles que l'on trouve dans des sociétés industrielles à l'international (c'est le cas des pétroliers par exemple) qui opèrent dans des pays à risque, où les enquêtes sont externalisées, et sont faites par des cabinets qui effectuent les enquêtes nécessaires. Il y a enfin les sociétés qui n'ont aucun service d'enquête, ni en interne ni en externe.

Comment les enquêtes se traitent-elles ? Les services d'enquête sont alimentés par des sources d'information diverses : cela peut être la délation : aux Etats-Unis, c'est un canal important ; cela peut être les constats du contrôle interne permanent ; cela peut être le résultat des audits (contrôles périodiques, audit interne, audit externe) ; cela peut être le hasard, des informations venant de l'extérieur, de la police, par exemple, etc.
Tout un ensemble d'informations arrivent dans les services d'enquête. Et qu'attend-on d'une enquête ? Qu'elle soit répertoriée et constitue un système d'information permettant ensuite de travailler sur des bases statistiques qui alimentent des réflexions sur les risques majeurs de la société dans le domaine de la fraude. S'il n'y a pas de système d'information, il n'y a pas de matériaux pour construire une analyse des risques.
On constate, notamment dans le monde bancaire, un certain nombre de pratiques tout à fait intéressantes. Chaque affaire fait l'objet d'une fiche traitée de manière informatique : évaluation économique avec notamment la durée de la fraude (plus la fraude est longue, plus l'impact économique est important) ; résultats sur l'enquête elle-même (quelles sont les responsabilités ?) ; traitement (qu'a-t-on fait ? y a-t-il un traitement RH, un traitement judiciaire ?). Les affaires ne sont closes que quand l'ensemble du processus est lui-même terminé.

Je suis convaincu que la structure des enquêtes et les structures d'information issues de ces enquêtes sont très utiles, ensuite, pour mener une analyse rationnelle, et alimenter des plans d'action structurés sur les risques de fraude.

Jean-Yves PELISSON

Vous avez beaucoup parlé des moyens et les enquêtes sont un moyen de lutte contre la fraude. Je voudrais à nouveau insister, parce que c'est la situation à laquelle nous avons été confrontés, il y a de cela maintenant dix-huit mois, sur les préalables qui conditionnent la réussite d'une action de lutte contre la fraude.
On a parlé tout à l'heure, en reprenant des termes anglo-saxons, de tone at the top. J'ai insisté sur l'importance de la définition, sur le fait que cette définition soit partagée par le management. Je pense qu'il n'y a pas de possibilité de réussir une lutte contre la fraude s'il n'y a pas une action résolue, éthique de sensibilisation, qui permette d'avoir un terreau sur lequel la fraude ne peut pas proliférer.
On peut développer tous les moyens que l'on veut, s'il n'y a pas un bon positionnement dès le départ, si l'on n'a pas un vrai soutien du management, comme une lettre du directeur général à l'ensemble de ses managers, insistant sur le fait que la lutte contre la fraude est une démarche sérieuse, prise en compte par le groupe, par le biais de la signature d'une charte de lutte contre la fraude ou par l'intégration à la charte d'éthique d'élé-

 © IFACI

ments relatifs à la fraude, si tout ceci n'est pas fait, les moyens que l'on développera ne permettront pas de tirer tous les bénéfices escomptés. De même, on peut faire toutes les campagnes de prévention que l'on veut, si l'on ne met pas ensuite en place des dispositifs de détection et de traitement approprié, les efforts seront vains.
Je voudrais revenir sur l'organisation d'AGF dans la lutte contre la fraude. Lorsque nous avons été amenés à traiter ce problème, pressés par les réglementations SOX, nous nous sommes posé la question de savoir comment opérer, et nous avons décidé de nommer un coordonnateur de la lutte contre la fraude. Dans un groupe de notre dimension (30 000 personnes dans le monde, 13 000 en France), il était possible d'envisager la nomination d'un responsable de la lutte contre la fraude, dont la première série d'actions a été le développement d'une charte dédiée à la lutte contre la fraude, des campagnes de sensibilisation, des dispositifs de formation diffusés par l'intranet, des campagnes d'affichage. Ce responsable est rattaché au directeur juridique du groupe, qui est également secrétaire général et en charge des fonctions de conformité. Il est totalement dissocié de la fonction audit.

Xavier BREGOU

Je ne vais pas contredire mon prédécesseur. Je suis en plein accord avec lui : si vous ne sensibilisez pas l'ensemble de vos collaborateurs, il n'y a aucune chance que le dispositif fonctionne.
Les statistiques américaines évaluent à 5 % du chiffre d'affaires le montant des fraudes dans les entreprises. En France, dans le secteur de la distribution, le montant des fraudes est de 2 % du chiffre d'affaires, ce qui n'est pas neutre.
Il y a deux ans, on a donc voulu sensibiliser l'ensemble des collaborateurs du groupe à ce problème. On a établi un diagnostic de la fraude au sein des entreprises de nos enseignes. Ce diagnostic n'avait qu'une seule vocation, c'était d'essayer de faire comprendre au *top management*, ce qu'est réellement la fraude. Pour certains d'entre eux, le vol, c'est de la fraude, le détournement d'actifs aussi bien sûr. Mais une fausse déclaration aux assurances, est-ce vraiment de la fraude ? N'est-ce pas, parfois, pour le bien de l'entreprise ?
Ce diagnostic nous a permis *in fine* d'établir une définition de la fraude, de construire un code de conduite des affaires et une charte d'éthique que nous avons diffusés à l'ensemble des collaborateurs du groupe. Cela s'est fait par une communication du comité exécutif du groupe aux présidents et secrétaires généraux des enseignes, lesquels ont adapté les règles en fonction des cultures de leurs entreprises. Tout collaborateur qui intègre le groupe aujourd'hui, se voit remettre un code d'éthique et un code de conduite des affaires. Il est informé et sensibilisé.

Nous avons mis en place une ligne éthique, qui n'est pas un *whistleblowing* à l'américaine. Les collaborateurs informés d'une fraude, ne sont pas tenus de prendre leur téléphone ou d'envoyer un e-mail via cette ligne éthique, mais ils savent qu'ils ont la possibilité de le faire ; libre à eux de le faire, en leur âme et conscience. Nous avons traité le *whistleblowing* à la française, qui permet des remontées, de temps en temps, de suspicions de fraude, de malveillances, etc.

La lutte contre la fraude chez PPR est très marquée dans la fonction achats qui est une fonction à risque. C'est pourquoi nous appliquons une politique uniforme dans l'ensemble de nos enseignes pour tous les acheteurs qui ne restent pas plus de dix-huit mois en poste sur leur typologie de produit. Nous considérons que, passé ce délai, des habitudes, des connivences peuvent naître, susceptibles de favoriser des fraudes.
L'audit interne examine, par le biais de ses missions, la problématique de fraude, mais il n'y a ni mission spécifique, ni programme de travail, sur la problématique de fraude. Nous ne sommes pas dans une culture anglo-saxonne. Nous y viendrons peut-être.

Noël PONS

Quand considérez-vous qu'une fraude est importante ou pas ? Est-ce qu'il y a un niveau significatif ?

Marc CHAMBAULT

Je pense qu'il n'y a pas non plus de seuil mathématique, dans le domaine de la fraude. C'est l'expérience et l'existence d'un système d'information structuré, comme on en voit dans les compagnies d'assurance ou les banques, qui permettent de connaître les affaires. Leur impact économique, leur durée facilitent des analyses du type Pareto.
Le seuil est celui que l'on peut proposer aux instances de gouvernance, un *reporting* significatif, de façon à ce que les administrateurs et le comité d'audit ne soient pas submergés d'informations secondaires et de petites affaires, mais soient informés des grands risques liés à l'activité de la société.
Quand j'étais directeur de l'audit du groupe France Télécom, je faisais remonter, tous les six mois, une dizaine d'affaires pour lesquelles il y avait un impact financier d'une certaine importance sur le fonctionnement économique du groupe ; une dizaine d'affaires, à rapprocher des centaines d'enquêtes faites dans le groupe pendant la même période.

Jean-Yves PELISSON

Pour ce qui nous concerne, l'approche est de même nature, néanmoins différenciée selon qu'il s'agit de la typologie que j'évoquais tout à l'heure de fraude à l'assurance où, là, on entre dans des volumes extrêmement élevés de polices d'assurance, et donc de détection par le biais de critères, d'indicateurs avancés qui permettent de repérer des secteurs où l'on pourrait se trouver confronté à la fraude.
Je distingue cette partie-là de la partie fraude interne qui correspond effectivement à des données statistiques beaucoup plus limitées en nombre et où nous appliquons une politique de remontée systématique des fraudes au premier euro, et même des fraudes avortées, pour une raison très simple qui est que nous tenons à analyser chaque scénario de fraude, même lorsqu'il n'y a pas de préjudice final, car finalement le fraudeur, en général, ne détourne que ce dont il a besoin : même si la brèche, dans le système d'information ou dans les procédures, permet de détourner 1 million, s'il n'a besoin que de 10 000 euros, le plus souvent, il détournera 10 000 euros.

Xavier BREGOU

Vous avez bien compris, je crois, que nous subissons un certain nombre de vols quotidiens en magasin. Seuls remontent au comité d'audit, qu'il s'agisse de la maison mère ou de nos branches, les cas significatifs, qui se comptent sur les doigts d'une main sur une année ; le reste est laissé à l'appréciation de chacun des managers ou patrons d'enseignes ou de filiales.

Noël PONS

Quel est le rôle de l'audit interne là-dedans ? Comment fonctionne-t-il ?

Marc CHAMBAULT

Je ne voudrais pas que l'on reste sur l'impression que je minimisais les opérations de sensibilisation et d'éthique, mais j'ai plutôt insisté sur l'aspect systèmes et traitement, parce que souvent, dans les entreprises, il y a un certain nombre de défaillances dans ce domaine.
Cela me permet de dire qu'un des rôles de l'audit interne, dans le cadre notamment de son positionnement vis-à-vis de la gouvernance, est, quand un code éthique existe, de s'assurer qu'il est diffusé à l'intérieur du groupe, qu'il est bien compris des salariés, qu'il est mis en œuvre de façon adéquate ; sachant par ailleurs que des chartes particulières ou sectorielles peuvent exister dans les métiers à risque. L'audit doit accompagner le déploiement de la sensibilisation au travers des référentiels que sont les chartes éthiques.

L'audit interne est un vecteur clé dans l'évaluation de la qualité du contrôle interne, en particulier dans le domaine des fraudes. Le plan d'audit doit intégrer des vérifications périodiques sur les processus clés mis en

 © IFACI

face des risques majeurs de fraude ; l'audit vérifiera que, dans les processus, les points clés liés à la fraude sont bien intégrés et décrits par les contrôleurs internes dans leur documentation. C'est un rôle fondamental de l'audit interne.

Jean-Yves PELISSON

En matière de lutte contre la fraude, l'audit interne a un rôle à jouer, mais la responsabilité première incombe au management.

Je considère que l'audit a trois rôles possibles à jouer.

Le premier est un rôle de facilitateur. L'exemple le plus classique est, dans le cadre d'une mission générale d'audit, de regarder ce qui est fait dans le domaine de la fraude au sein de l'organisation et, si l'on constate que l'on n'en fait pas suffisamment, d'émettre des recommandations à destination du management indiquant qu'il est primordial d'agir en la matière. L'audit est donc celui qui sensibilise au fait que le risque global de fraude est sous-estimé dans l'organisation, et qu'il est important de pallier cette insuffisance. L'audit peut établir un état des lieux pour déterminer les actions à mettre en œuvre et l'organisation à mettre en place ; il peut, dans ce cadre, jouer un rôle de conseil pour proposer une organisation. Une fois que cette organisation est en place, il retrouve son rôle d'auditeur.

Le deuxième rôle, me semble-t-il, une fois le dispositif mis en place, est de conserver un rôle d'acteur, par exemple dans le domaine de l'investigation. Dans certaines organisations, il y a même des équipes d'investigation, lorsque la taille des activités le justifie, qui sont intégrées dans les directions d'audit. Dans d'autres organisations – on le voit aux Etats-Unis de plus en plus – l'investigation tend à se détacher de l'audit, en raison des exigences d'objectivité et d'indépendance de l'audit qui font qu'on ne souhaite pas faire cohabiter les deux.

Le troisième rôle, dans lequel je me sens plus à l'aise, est celui de superviseur, qui considère le dispositif de lutte contre la fraude comme un objet d'audit, donc comme un élément qui figure dans le plan pluriannuel d'audit ; et, tous les deux ou trois ans, l'audit procède à une évaluation du dispositif de lutte contre la fraude avec l'ensemble de ses composantes.

A partir du moment où ces trois choix sont possibles, il faut que le positionnement adopté par l'audit soit clair et sans ambiguïté, et que chacun comprenne bien le rôle joué par les acteurs du dispositif et par l'audit lui-même.

Dans l'organisation d'AGF, l'audit centralise le *reporting* des fraudes parallèlement au coordonnateur de la lutte contre la fraude. L'audit procède ponctuellement (avec un auditeur spécialisé) à des audits « post-mortem » : six mois après la réalisation d'une fraude, nous vérifions que la fraude a été traitée par les équipes en charge du traitement de la fraude, que les mesures correctives ont bien été mises en œuvre. Nous intégrons la fraude dans nos programmes de travail, lorsque nous faisons l'audit de telle ou telle direction, au même titre que les dispositifs de la CNIL ou du blanchiment.

Xavier BREGOU

Chez nous, l'audit interne est avant tout un accompagnateur sur la problématique de la fraude. Nous sommes là pour accompagner le management, pour le sensibiliser (ce qui a été fait, comme je vous l'ai dit), lui faire part des problématiques et des informations, afin que nous puissions – et là, c'est la deuxième composante que je voulais évoquer avec vous – dans le cadre de missions d'audit ou de contrôle interne, remédier à toutes les défaillances, et limiter ainsi au maximum la fraude.

© IFACI

Il nous arrive de diligenter quelques missions d'investigation sur des fraudes importantes aux yeux du groupe PPR pour essayer : 1) de les comprendre, 2) de les traiter, 3) de mettre en place une organisation pour éviter que cette typologie de fraude se répète dans le futur. Mais c'est une partie relativement faible de notre activité.

© IFACI

BIBLIOGRAPHIE

- Audit et Fraude – Noël Pons et François Vidaux – IFACI – février 2004
- Cols blancs et mains sales – Noël Pons – Ed. Odile Jacob – mars 2006
- Halte aux fraudes – Olivier Gallet – Ed. Dunod – février 2005

* * * *

* * *

* *

*

Conception - réalisation : EBZONE Communication (eblanc@ebzone.fr)

© IFACI