ifaci

institut français de l'audit et du contrôle internes

En partenariat avec

ACL™

Actes du colloque

Gouvernance et maîtrise du risque de fraude

mardi 17 novembre 2009

Cercle National des Armées

Colloque

En partenariat avec ACL

Gouvernance et Maîtrise du risque de fraude

Mardi 17 novembre 2009

Sommaire

PRESENTATION DU PROGRAMME PAR JEAN-FRANÇOIS SAUTIN 3

L'ACTUALITE EN MATIERE DE FRAUDE : AFFAIRE MADOFF, ESCROQUERIES SUR LE MARCHE DE LA FINANCE CARBONE, UTILISATION FRAUDULEUSE DES MOYENS DE PAIEMENT, LES FRAUDES RECENTES AURAIENT-ELLES PU ETRE EVITEES ? PAR NOËL PONS 4

COMMENT FORMER ET SENSIBILISER LES OPERATIONNELS A LA FRAUDE ? 9

QUESTIONS/REPONSES 17

COMMENT CONSTRUIRE UNE CARTOGRAPHIE DES RISQUES LIES A LA FRAUDE ? 22

L'ANALYSE DES DONNEES : RETOUR D'EXPERIENCE DE L'UTILISATION DU LOGICIEL ACL POUR DETECTER LES RISQUES DE FRAUDES PAR GERARD VILLARD 30

QUESTIONS/REPONSES 34

TABLE RONDE : LE PROCESSUS DE CERTIFICATION : QUELS EN SONT LES PRE-REQUIS ? 36

ANIME PAR NOËL PONS, *CONSULTANT ;* .....
AVEC FREDERIC GEOFFROY, *RESPONSABLE AUDIT INTERNE, SGCIB ;* .....
MARIANO MARCOS, *ASSOCIE, PRICEWATERHOUSECOOPERS ;* .....
HELENE PLOIX, *PRESIDENT DE PECHEL INDUSTRIES PARTENAIRES, PRESIDENT DE COMITES D'AUDIT ;* .....
JEAN-FRANÇOIS SAUTIN, *SENIOR VICE-PRESIDENT GROUP AUDIT, LAFARGE ;* .....
QUESTIONS/REPONSES 47

QUELS ENSEIGNEMENTS PEUT-ON TIRER DE L'AFFAIRE KERVIEL ? PAR JEAN-BAPTISTE GIROS 49

1. Les principaux mécanismes de la fraude 49
2. Le rôle du contrôle périodique dans les investigations 51
3. Les enseignements pour le dispositif de contrôle périodique 52

Questions/Réponses 53

QUELLE EST LA RESPONSABILITE DE L'AUDITEUR INTERNE LORS DE LA CONDUITE D'UNE MISSION ANTI-FRAUDE ? PAR SYLVIE LE DAMANY 57

Questions/Réponses 59

PRESENTATION DU PROGRAMME PAR JEAN-FRANÇOIS SAUTIN

Senior Vice-President Group Audit, Lafarge

Je vous accueille avec plaisir à ce nouveau colloque de l'IFACI sur la fraude, thème qui est, malheureusement, de plus en plus d'actualité.

Je suis directeur de l'audit interne dans le groupe Lafarge, mais je ne suis pas un expert de la fraude. Je suis, comme beaucoup d'entre vous, venu aujourd'hui pour améliorer mes connaissances et ma compréhension du sujet. Je pense que nous sommes tous confrontés au défi d'être davantage proactifs que réactifs dans le domaine de la fraude. Les intervenants, ce matin et cet après-midi, vont nous aider à creuser le sujet, et à profiter de leur expérience et de leurs conseils.

L'IFACI a engagé deux Cahiers de la recherche sur la fraude, sur le rôle de l'audit interne et du contrôle interne en matière de fraude. Un premier Cahier, pratiquement terminé, a été réalisé par le groupe des responsables financiers ; le deuxième Cahier, pour lequel j'ai accepté la présidence, concerne les industries, les commerces et les services.

Quand on demande aux intervenants d'un Cahier de recherche de définir la fraude, on constate une diversité de définitions, car les entreprises ont des approches et des regards un peu différents. Plusieurs définitions, donc, mais en fait, un même fil conducteur. La définition arrêtée par le Cahier de la recherche financier, c'est-à-dire par des personnes proches du monde de la finance et des banques, est courte, concise, et est en ligne avec les définitions de l'IFACI et de l'IIA. Il faut souligner trois éléments importants : le caractère volontaire de la fraude, la tromperie et le gain recherché par le fraudeur. Dans certains cas, il peut y avoir fraude sans gain matériel pour le fraudeur, si ce n'est le « gain » un peu pervers de nuire à l'entreprise.

Il faut aussi souligner la très grande créativité et l'imagination très fertile des fraudeurs dans des domaines infiniment variés. Il y a beaucoup d'intelligence et de ruse dans l'esprit de beaucoup de fraudeurs, et c'est un défi incessant : il nous faut sans cesse renforcer les structures, les contrôles, etc., et être bien conscient que toute faille, toute lacune d'un système sera exploitée par le fraudeur.

Pour nous parler de l'actualité en matière de fraude, je vais appeler Noël Pons, qui est ancien conseiller au Service central de prévention de la corruption, et auteur de nombreux ouvrages et articles portant sur la fraude et la criminalité.

L'ACTUALITE EN MATIERE DE FRAUDE : AFFAIRE MADOFF, ESCROQUERIES SUR LE MARCHE DE LA FINANCE CARBONE, UTILISATION FRAUDULEUSE DES MOYENS DE PAIEMENT, LES FRAUDES RECENTES AURAIENT-ELLES PU ETRE EVITEES ? PAR NOËL PONS

Consultant

La fraude, quoi de neuf ? Rien. Si ce n'est une multiplication des problèmes.
Rien de neuf, tout simplement parce que les montages les plus récents existent depuis des siècles, pour la plupart d'entre eux. La seule nouveauté, qui est essentielle, est le fait de la technologie, des modèles mathématiques, de l'informatique, qui rendent extrêmement difficile le contrôle de ces opérations.

On parle souvent des montants des fraudes. Il est difficile de préciser ces montants, puisqu'ils sont par définition cachés. On impute à Madoff 47,8 milliards d'euros. Mais l'on commence à penser que ce montant pourrait être majoré d'une dizaine de milliards qui se promènent on ne sait trop où.
Calixte (247 après J.-C.), était un Romain qui a monté, d'une certaine façon, la première escroquerie sur du financier. Il a été mis en prison. Il était chrétien et comme – ainsi que le voulait à l'époque la religion catholique – on pardonnait les offenses, il est devenu pape. Et c'est lui qui, le premier, a proclamé l'interdiction aux catholiques de faire des prêts à gage. Après la fraude, la rédemption.
Ponzi (1920) et son système de cavalerie ; Stavisky (1930), prince de l'escroquerie. Aucun des deux n'a rien inventé. C'est une très vieille histoire toujours revisitée. C'est tout simplement faire payer par des nouveaux clients les sommes que l'on doit aux anciens.
Le principe, vous le connaissez, il est basé sur la sottise, ou plutôt la crédulité : on croit que l'on va faire une bonne affaire. On croit la personne qui vous propose des placements exceptionnels, « mais surtout, ne le répétez pas, puisque ce sont des placements qui ne concernent qu'une élite. »
L'appât du gain, bien évidemment, puisque derrière toute cette opération se crée, en filigrane, une problématique de dissimulation fiscale et de blanchiment, puisque après ces opérations, on entre dans des trusts, dans des opérations assez complexes. Le problème, ce sont les trous réglementaires qui existent dans ce domaine. Les trous réglementaires (par exemple pour un pays comme la France, qui a une réglementation particulièrement cohérente – il y a d'ailleurs assez peu de personnes qui se sont fait prendre avec du Madoff –) peuvent être identifiés dans ce que l'on appelle le ratio poubelle : il est interdit de vendre un produit dès l'instant que tous les éléments ne sont pas évalués, à l'exception d'un pourcentage que les structures européennes ont permis d'intégrer.
Ces ratios poubelle font que, si vous achetez des SICAV sans être au courant de l'opération, vous allez simplement tout perdre parce que, la fausse monnaie chassant la bonne, votre SICAV va perdre la totalité de sa valeur puisque l'on sait qu'elle est infectée. Et une fois qu'elle est infectée, il n'y a pas de moyen de contrôle.
Parmi les termes que l'on utilisait pour qualifier ces SICAV que l'on vendait à des entreprises ou à des personnes de bonne foi, il y en avait une qui s'appelait le « monétaire tilté », comme le « tilt » des machines à sous. Il y a aussi les qualifications un peu atypiques – rappelez-vous Enron, avec la Guerre des étoiles – et un glissement vers d'autres comptabilisations globales. Cela veut dire qu'en fait, au bout d'un moment, il n'y a plus aucun système de contrôle.
Le système Madoff était assez simple : des courtiers, des filiales, des fonds nourriciers, la famille, et une fausse comptabilité. Il a d'ailleurs été très surpris de ne pas être découvert avant 2008. Et les gens n'étaient pas méfiants, puisqu'il avait fait l'objet de sept vérifications, aucune d'elles n'ayant porté sur les écritures comptables, soit dit en passant ; seuls les mails étaient vérifiés. Cela démontre peut-être un problème dans la formation des personnes qui effectuent des recherches.

Il y a actuellement une cinquantaine de Madoff qui se promène dans le monde. Un avocat, Dreyer, laisse un trou de 400 millions de dollars. Il émettait des faux billets à ordre tirés sur une vraie société ; et cela marchait. C'est assez étonnant.
Les réseaux de fonds nourriciers soulèvent des problèmes. Certains gérants de patrimoine ont attaqué les banques sur ce point.
On se trouve confronté à une défaillance conjointe du contrôle interne et du contrôle externe. Se pose alors la question : comment analyse-t-on la trésorerie ? On ne peut pas, on n'a pas pu contrôler la nature de ces opérations : c'est quand même l'essentiel, la base. Peut-être y a-t-il une recherche à faire d'une nouvelle analyse de la trésorerie. Mais chaque fois que l'on analysera la trésorerie, on devra bien évidement la coupler avec les immobilisations financières et avec la problématique des dérivés. Donc, nouveau chantier pour les problématiques de fraude.

Les affaires d'initiés : à partir d'informations relevant du terrorisme, des écoutes ont été mises en place (d'après ce que dit la presse). On s'aperçoit que ces écoutes travaillent sur le terrorisme mais aussi que des informations et des délits d'initiés sont développés autour d'un fonds. Ce n'est pas étonnant : la nature d'un fonds est justement de disposer d'informations qui ne sont pas toutes des délits d'initiés, mais il est obligatoire d'avoir des informations particulières puisque, lorsque l'on a un fonds, on va chercher non pas telle et telle valeur, mais la tendance de la valeur. Cette tendance, on l'a par quoi ? Par des connaissances, par des analyses, par des appels téléphoniques aux clients, aux fournisseurs. En fin de compte, il y a toujours une recherche d'information qui relève d'ailleurs de l'intelligence économique.
Cinq dirigeants de sociétés ont été impliqués, dont l'une, assez paradoxalement, vendait un logiciel qui permettait d'identifier les délits d'initiés ! Je ne sais pas si le logiciel fonctionnait mal, si on ne l'avait pas acheté, s'il y avait un autre problème, ou peut-être avait-on trop bien analysé le problème et l'on s'était aperçu de la facilité de jouer. Là-dessus, que va-t-on faire ? On va tirer profit de données confidentielles et on va gagner de l'argent en toute illégalité.
Il y a eu là aussi un problème lié aux écoutes. Comme dans les affaires Madoff de 2008, les financiers ont été écoutés et le procureur américain déclarait : « Maintenant, il faut savoir que les gens qui gèrent des fonds sans scrupule peuvent être écoutés comme les criminels mafieux. » Cela va déboucher sur des informations. Finis les mails. On a vu, avec les affaires Enron et Worldcom, que le relevé des mails pouvait donner des informations. Cela avait été corrigé par les fraudeurs. Et l'on passe actuellement à un niveau supérieur, ce qui veut dire que de nouvelles méthodologies vont se mettre en place.
On disait que Madoff connaissait parfaitement la SEC, qu'il connaissait le NASDAQ, et qu'il ne pouvait donc pas ne pas avoir d'informations. Et c'est pour cela qu'on lui faisait confiance. On est donc toujours dans le cadre du délit d'initiés.
L'investigation qui se rapproche de la grande criminalité, c'est une évolution qui devient incontestable sur toute cette problématique de jeu.

Les « bouilloires » sont une autre technique. Celui qui explique le mieux cette technique, c'est Zola, dans l'Argent. Vous voyez qu'on n'a rien inventé. Un Tycoon a tout simplement manipulé ses actions pour les faire passer de 5 à 55 euros, cela veut donc dire un gain de 50 euros par action : vente, jeu en bourse, récupération des fonds. Gestionnaire de banque privée, il a vendu sa holding et tout cela a disparu dans des comptes suisses.
Il y a aussi l'intoxication par une communication manipulée. Il est nécessaire de donner des informations à la presse spécialisée, sans bien évidemment expliquer la réalité des opérations, puisqu'elle ne suivrait pas. Mais il y a tout de même une réelle simplicité dans l'analyse.
Prenons le montage suivant : un trader a réalisé une opération assez intéressante, au mois d'août dernier. Il a joué sur le pétrole, et a acheté sur des bases qui dépassaient la valorisation des réserves pétrolières mondiales. Cela aurait dû étonner tout le monde. Eh bien, pas du tout : tous les traders se sont jetés sur cette opération et ont joué à la hausse sur ces réserves. Cela veut donc dire que l'on ne contrôle même pas la réalité, le fond de l'opération. Cela devient très inquiétant.

Les bouilloires font monter la valeur. On « récupère » le maximum de personnes dans ce type d'achat, le problème étant de quitter le bateau le plus vite possible avant que les parts ne redescendent. Dans une entreprise, aux Etats-Unis, les gérants sont poursuivis pour ce type d'opération, et pour une centaine de millions de dollars détournés. Comme pour les Ponzi, ces bouilloires très anciennes sont toujours d'actualité.
Tous ces montages fonctionnent sur des bases mathématiques et sur un système informatique.

Le vol de code source. Un cas est dans la presse. Il s'agit d'une personne qui travaillait sur l'informatique, dans une grande banque, et qui a été mise en examen puis libérée moyennant une caution de 150 000 dollars. Elle avait dérobé les codes source permettant à la plate-forme d'échanges entre acheteurs et vendeurs de travailler. L'emploi du système XBRL ne permet pas de contrôler totalement ces opérations qui ont été transférées en quatre envois dans les pays de l'Est. Pour l'instant, les opérations sont arrêtées ; on ne sait pas ce qui a pu se passer, mais la personne est poursuivie.
Autre exemple : un trader est parti, de la même banque, d'ailleurs, et il est poursuivi pour avoir emporté le système mathématique d'évaluation qui permet de donner, avec quelques minutes d'avance sur la concurrence, la tendance de l'évolution des valeurs. D'où une probable manipulation des coûts.

Le scandale carbone. Vous avez bien sûr entendu parler de la taxe carbone. Lorsqu'une société pollue, elle peut acheter des droits à polluer d'une autre société. Ces droits à polluer se valorisent et entrent dans l'actif des bilans. Certaines sociétés ont 30 % de leur actif constitué par ce type de droits.
Dans mon dernier livre, « Arnaques », je posais le problème de ce type de montage, dans la mesure où je ne conçois pas, en termes de fraude bien sûr, comment on peut évaluer ce type de droits. Et je réussis mal à l'intégrer en comptabilité, si ce n'est en forçant l'entrée.
D'une certaine façon, l'histoire m'a donné raison : un certain nombre de traders désœuvrés, liés à la criminalité, à Londres, ont profité du fait qu'il n'y avait pas de taxe à la valeur ajoutée en Angleterre sur ces valeurs et qu'il y en avait dans les autres pays d'Europe. Résultat : ils ont fait monter des circuits de fausses factures, des carrousels de TVA, tout simplement. Et ils ont détourné environ 40 millions d'euros sur ces opérations, ce qui a entraîné la suspension de la TVA sur tout le système.
Vous constatez que, dans un domaine complexe, dans un domaine écologique, dans un domaine qui est très positif pour tout le monde – le carbone est une valeur verte –, il se trouve des personnes qui trouvent le moyen de frauder par le biais de montages très compliqués. Il s'agit là d'un détournement par la criminalité.
Comment ces fraudes ont-elles été découvertes ? Tout simplement parce que l'on s'est aperçu que le BlueNext, le système de contrôle et de transaction des valeurs carbone, augmentait de manière inconséquente. Cela veut donc dire que, dans ce domaine, il y a une possibilité de contrôler, à la condition que l'on regarde au bon endroit et au bon moment.
Un autre exemple : l'escroquerie du sucre. C'est tout simplement un circuit de détournement de taxes européennes entre Bruxelles, l'Ukraine et la Croatie : fausses factures, faux documents, toujours le même système. On entre dans un autre domaine qui ne concerne pas forcément l'activité d'une entreprise, mais qui concerne la manière dont on « tunnellise » les problèmes.

Les réseaux organisés et les moyens de paiement.
L'escroquerie des *miles*, vous en avez entendu parler, c'est sorti dans la presse. Vous savez que, lorsque vous voyagez, vous disposez de *miles* en fonction des voyages que vous faites et vous pouvez les réutiliser à titre personnel, par la suite. Il se trouve que, en raison d'une faible sécurisation des données et des contrôles d'authentification, un certain nombre de personnes ont pu avoir accès à ce stock de *miles* et les utiliser à titre personnel. De ce que l'on sait aujourd'hui, le montant des détournements par personne était de l'ordre de 400 000 euros, ce qui représente une valorisation extrêmement importante, et peut poser un problème d'image pour l'entreprise.

Dans le même registre, les détournements de virements, par obtention de codes, et se fondant sur une carence du contrôle. Il s'agit de détournements de virements informatisés, et c'est pourquoi, pour certains virements complexes, on préconise un rappel – soit téléphonique, soit par mail sécurisé – de la personne qui donne l'ordre de passer. Il s'est créé, depuis quelques mois, une sorte de méthode de contrôle dans laquelle on fait la moyenne des virements de telle entreprise sur tel pays et, dès l'instant où un virement n'est pas dans le cadre d'un pays reconnu comme valide ou qui sort de la moyenne des montants, on bloque le virement pour éviter un détournement de la somme.
Le vol des billets par un transporteur de fonds. On aurait pu s'intéresser à son train de vie : il roulait avec une Audi A8 et, accessoirement, avec une Maserati. Cela veut dire que quelqu'un qui gagnait 1 700 euros par mois avait une voiture trois fois plus chère que celle du gérant ou du directeur de la société. C'est un indice.
Autre problème de contrôle : dans le sud de la France, une personne qui approvisionnait les DAB, faisait une demande pour 350 000 euros, et elle en laissait 100 000 dans le distributeur. Calculez la différence : il y en avait 250 000 pour elle à chaque fois ; elle a détourné un million et s'est envolée.
Ces quelques exemples montrent qu'il y a des éléments simples à prendre en compte. Il existe des indicateurs, comme en matière d'intelligence économique, d'ailleurs. La recherche de fraude est très proche de l'intelligence économique. 90 % des éléments susceptibles d'éveiller un soupçon de fraude, de blanchiment, sont dans les comptes, mais il faut savoir où ils se trouvent, il faut savoir comment aller les chercher et il faut savoir comment on les fait remonter.

De ces exemples, quelles leçons doit-on tirer ?
D'abord, douter de tout : les cadeaux, pas forcément matériels, les bons coups, les bonnes idées, les tuyaux, ce n'est plus de mise actuellement. Si l'affaire est trop intéressante, il y a des chances qu'elle soit pourrie. La bonne affaire, il faut l'analyser avec beaucoup plus de soin qu'une affaire moins risquée.
Tenir constamment à jour la cartographie des risques. Dresser l'historique. La difficulté est que chaque entreprise, chaque secteur a sa propre typologie. L'intérêt est donc de dresser l'historique des affaires qui ont eu lieu dans chaque entreprise. Pourquoi ? Parce que, à coup sûr, une affaire qui s'est déroulée il y a dix ans, va se reproduire pour des raisons diverses. Ne perdez pas de vue que, lors des fusions, des regroupements, pendant un an et demi environ, il est possible de frauder pratiquement sans aucun risque, et sur des montants extrêmement importants. La cartographie, cela veut donc dire avoir un historique, le distribuer aux auditeurs et aux contrôleurs, mais aussi essayer de comprendre ce pour quoi il n'y a pas d'explication : souvent, lorsqu'une opération ne s'explique pas, lorsqu'elle est trop complexe, trop difficile à comprendre, les risques de fraude sont très présents.
Disposer des ressources nécessaires : c'est peut-être l'élément le plus novateur. Le besoin de spécialistes (juristes, fiscalistes, informaticiens…) se fait de plus en plus sentir que ce soit à l'audit interne ou externe. La fraude touche à tous les domaines. On a besoin également d'un personnel stable, qui ne reste pas trois ans dans un poste, et qui soit capable d'utiliser les méthodes semi-informatisées ou informatisées, permettant d'identifier des masses de remontées.
Chercher à contrôler les petites fraudes. Comme vous le savez, globalement, 20 % des gens frauderont toujours, 20 % ne frauderont jamais et 60 % peuvent basculer. Si vous gérez bien et si vous faites peur aux fraudeurs potentiels qui ne sont pas suffisamment résolus pour entrer dans un montage, vous avez déjà gagné la partie, ne serait-ce que sur l'image.
Savoir perdre du temps pour examiner tous les détails. Il faut du temps, il faut des moyens et la recherche de la fraude a un coût.
Et le plus important : savoir le faire savoir ! Dire ce que l'on fait. Chaque fois que l'on a décelé une fraude, on explique, on développe, on diffuse. Une bonne communication est primordiale dans ce domaine.

Jean-François SAUTIN

Ce qui m'a particulièrement intéressé, c'est le $C0_2$. En effet, dans un groupe cimentier, on est confronté à toute la problématique émergente du trading de $C0_2$ et j'avoue que nous n'avions pas réfléchi particulièrement aux possibilités de fraude sur ce trading. Vous avez abordé beaucoup de sujets surtout dans la dernière partie de votre exposé. Vous avez parlé du poids croissant de la technologie, des spécialisations, etc. Comment arrive-t-on à créer une chaîne vertueuse à partir de doutes, de bon sens, de contrôles… ?

Noël PONS

Comment fait-on ? C'est là toute la difficulté. Il faut d'abord penser que le problème existe. C'est le premier point. Par exemple, sur le $C0_2$, une méthode classique, qui n'est pas tout à fait une méthode de fraude, parce qu'elle peut se justifier, non pas sur le trading mais sur une méthode d'équivalents de même nature. Vous avez une entreprise, en France, qui pollue peu. Vous allez donc avoir un coût important pour un gain limité. Par contre, si vous avez une entreprise en Ukraine, qui pollue beaucoup, vous allez acheter l'entreprise d'Ukraine. On a appris ainsi qu'un certain nombre de mafias des pays de l'Est ont acheté des vieilles usines pour un rouble et les ont revendues à des entreprises européennes, tout simplement parce que ces entreprises permettent d'avoir un bilan.
Jusqu'à quand cela va-t-il marcher ? Quelle est la valeur ? Comment analyse-t-on cette opération ? Vous voyez, c'est une situation qui ne pose pas a priori de problème, puisque l'entreprise existe bien ; cela devient un problème quand l'entreprise n'existait pas, qu'on l'a créée, que l'on a mis de vieilles maisons effondrées sur la photo, avec un grand tuyau, que l'on a ajouté trois personnes qui font semblant de travailler. On vous vend cela. Cela veut donc dire qu'au bilan, vous n'avez rien, vous avez du vent.
Il faut être attentif. Il faut surtout essayer d'être attentif à tout ce qui est étonnant, tout ce que l'on ne comprend pas : tous ces éléments, pourquoi est-ce que cela fonctionne ainsi ? De toute manière, la fraude émane de l'homme, d'un homme ou de plusieurs hommes, mais ce n'est que cela. Il n'y a donc qu'un homme qui pourra la traiter.
Il faut d'abord sentir l'opération, ensuite l'analyser et surtout rajouter, par exemple à un certain nombre d'audits, un pourcentage relié à la fraude, vérifier si ce processus n'a pas généré une perte, et faire remonter toutes les pertes, donc refaire de l'historique de ces opérations.
C'est pragmatique, il n'y a pas de réelle méthode, et si on vous dit le contraire, on vous ment. C'est vraiment de l'humain sur de l'humain. Et après, ma foi, bonne chance, comme on dit.

Jean-François SAUTIN

J'invite Marc Fourrier et Philippe Great à me rejoindre, pour nous parler de la formation et de la sensibilisation des opérationnels à la fraude.
Marc Fourrier est directeur de la conformité d'Allianz France, qui comprend notamment la lutte antifraude.

COMMENT FORMER ET SENSIBILISER LES OPERATIONNELS A LA FRAUDE ?

Marc FOURRIER, *Directeur de la conformité, Allianz France*

Philippe GREAT, *Responsable Sécurité financière, Groupama Banque*

Marc FOURRIER, *Directeur de la conformité, Allianz France*

C'est un sujet tout à fait en amont des dispositifs opérationnels globaux anti-fraude dont nous allons vous parler, mais c'est également un sujet permanent tout au long de la vie du dispositif anti-fraude. Nous allons alterner la présentation avec Philippe.

Jean-François SAUTIN

Philippe a sous sa responsabilité le service Sécurité financière de Groupama Banque.

Marc FOURRIER

Le groupe Allianz est l'un des acteurs principaux mondiaux en matière d'assurance et de services financiers et détient un certain nombre de filiales bancaires. Il est présent dans plus de soixante-dix pays. La partie française représente le deuxième marché pour Allianz, le premier étant l'Allemagne ; c'est donc une filiale qui contribue de façon significative au résultat du groupe. 15 000 collaborateurs en France, plus 6 000 distributeurs, des salariés, des agents généraux et également un réseau de courtiers. C'est important dans le dispositif anti-fraude, vous allez le voir.
Noël Pons remarquait que les risques de fraudes sont importants lors des fusions. Allianz France est issu de la fusion de 3 groupes (AGF, Allianz et une partie d'Athena) au début des années 2000. Aujourd'hui nous sommes à 100% Groupe Allianz et la marque AGF devient Allianz en France.
En 2004, Allianz étant coté sur les marchés américains, nous avons été soumis aux obligations de *compliance* Sarbanes-Oxley, ce qui nous a permis de mettre en place un programme qui est aujourd'hui la base de notre système de contrôle interne avec l'identification par processus des risques, des dispositifs de contrôle, dans le cadre d'une approche structurée. A cette occasion, nous nous sommes rendu compte que le dispositif anti-fraude présentait quelques lacunes. Cette insuffisance a été confirmée l'année suivante par un cas de fraude significatif médiatisé. Nous sommes loin des chiffres de Madoff, mais quand un agent général détourne plusieurs millions d'euros et que l'information passe sur TF1, c'est fâcheux pour notre image.
La direction de l'audit a mené une revue de façon à mieux comprendre ce qui se faisait en matière de fraude dans le groupe, de façon transverse, dans toutes les entités et les filiales. Je parle essentiellement de la fraude interne. Pour ma part, je ne parlerai pas de la fraude externe qui concerne essentiellement la fraude à l'assurance, qui est un sport national et international, et qui est davantage traité dans le cadre des processus d'indemnisation, par exemple.
Sur la fraude interne, notre dispositif était plutôt réactif : quand cela arrivait, on traitait, mais on n'était pas forcément bien organisé en matière de prévention pour l'éviter, ou de détection, de façon à minimiser les risques.
Cela nous a amenés, en 2006, à créer la coordination de la lutte anti-fraude (la CLAF), logée au sein de la direction juridique. Il y a eu un long débat pour savoir où l'on devait loger ce type d'organisation. Je vous passerai les débats mais, dans le groupe Allianz, il n'y a pas de dogme. Dans d'autres entités, la coordination de la lutte antifraude peut en effet dépendre du *risk management* ou de l'audit. J'ai mis en place le dispositif, ainsi qu'une politique anti-fraude, une politique de prévention, de détection, de traitement et de remédiation. En 2009, a été créée la direction de la conformité au sein de la direction juridique et conformité : la lutte antifraude a rejoint les autres blocs que j'anime, qui sont l'anti-blanchiment, l'anti-terrorisme, les lois informatique et libertés, et

un certain nombre d'autres sujets de *compliance*, à commencer bien sûr par l'éthique et la déontologie.

Philippe GREAT, *Responsable Sécurité financière, Groupama Banque*

Groupama Banque est la banque de Groupama, première mutuelle d'assurance en France : 16 millions de clients à travers le monde, 39 000 collaborateurs. Groupama Banque a près de 500 000 clients, une offre commercialisée par 2 200 agences Groupama, 1 000 agents généraux de GAN Assurances et 650 mandataires de Gan Patrimoine. On dispose de deux plates-formes téléphoniques pour gérer les appels clients et la commercialisation des produits ; nos collaborateurs sont au nombre de 700.

Groupama Banque est née de la fusion des deux entités bancaires de Groupama, la banque Finama et Groupama Banque. Il a été alors décidé de mettre en place un dispositif centralisé de pilotage, de coordination et de contrôle du dispositif de lutte contre la fraude, qu'elle soit externe ou interne.
A noter que cette démarche ne démarre évidemment pas en 2009, puisque la fraude était traitée, de manière décentralisée, dans les deux entités bancaires auparavant. Mais il a été jugé judicieux de créer, au sein du département conformité et contrôle permanent (rattaché à la direction générale), un service sécurité financière dont j'ai la charge, qui met en œuvre le pilotage, la coordination, le contrôle du dispositif de lutte contre la fraude, mais aussi le dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme. Nous verrons que ces deux problématiques sont souvent liées et que, d'une certaine manière, il est important de traiter les deux, sans perdre de vue l'une et l'autre.
Afin d'être plus efficace, le dispositif de lutte contre la fraude est totalement intégré au dispositif de contrôle interne.
Le dispositif s'accompagne de la mise en œuvre d'une politique de lutte contre la fraude qui repose sur quatre axes principaux : la prévention, la dissuasion, la détection, le traitement. Chaque étape du dispositif a un impact sur les différentes fonctions opérationnelles de l'organisation.

Pour pouvoir mettre en place un dispositif efficace de lutte contre la fraude, il faut d'abord **agir sur les comportements et mettre en place une organisation adaptée**. On va donc identifier et évaluer les risques de fraude ; on établira une cartographie spécifique de ces mêmes risques ; on mettra au point des procédures et une organisation permettant d'encadrer efficacement les collaborateurs ; on disposera bien sûr d'un plan de contrôle ; on assurera la confidentialité des procédures de contrôle ; on sensibilisera et formera les collaborateurs, mais aussi les prestataires et les clients sur les risques de fraude ; on développera une culture éthique au sein de l'entreprise ; on communiquera sur le risque de fraude au sein de l'entreprise ; on favorisera la rotation des postes. Je rappelle que la fraude, c'est l'affaire de tous, et non pas d'un individu ou d'une organisation.

En bref, il s'agit de **définir, expliquer et convaincre**. Ces points sont très liés. Ensuite, une fois que l'on a agi sur les comportements et que l'on a mis en place un dispositif, il va falloir dissuader, c'est-à-dire empêcher la fraude de se produire. C'est là qu'intervient la communication. La communication est primordiale : communication sur les risques encourus et les sanctions appliquées (sanctions générales, sanctions pénales), pour que les collaborateurs et l'ensemble des personnels du dispositif comprennent bien comment ils se situent, la portée de leurs actes…
Il faut disposer de clauses contractuelles, d'un règlement intérieur et d'un code de déontologie : c'est fondamental.
Il faut faire appliquer le plan de contrôle et les procédures : il ne sert à rien de mettre en place des beaux plans de contrôle et de définir des belles procédures si, ensuite, on ne s'assure pas de leur mise en application à la fois par les collaborateurs et les managers.
Il faut mettre en place des outils et des procédures de permission : l'informatique permet de bloquer certaines opérations dans les systèmes d'information, de mettre en place des doubles validations, des contrôles d'accès, qu'ils soient physiques ou logiques. La séparation des tâches est un des points

fondamentaux du dispositif. Les transactions doivent être enregistrées, ainsi que les confirmations, les limites. Les contrôles a priori et a posteriori doivent être mis en place dans une organisation la plus précise possible.
Tout cela se résume en deux mots : superviser et encadrer.

Agir sur les comportements, **empêcher ou tenter d'empêcher la fraude de se produire**, n'est malheureusement pas suffisant, il faut aussi être capable de la détecter. On va donc reconnaître si une fraude a eu lieu. Comment cela ? A partir d'indicateurs d'alerte (traces informatiques, accès aux locaux) ; en réalisant des reportings réguliers ; en établissant un dispositif d'alerte éthique, qui permettra aux collaborateurs de faire remonter des informations, lesquelles peuvent concerner des fraudes externes (fraudes clients, par exemple), mais aussi des fraudes internes (actes de malveillance ou autres) ; en disposant d'outils de détection et d'alerte a priori et a posteriori : si c'est a priori, tant mieux, cela veut dire que l'on a pu détecter une fraude avant qu'elle ne se concrétise, mais hélas, c'est rare, d'où la nécessité de mettre en place des mesures a posteriori, mais au plus près de l'acte ou de la réalisation de la fraude.

Comment répondre à un cas de fraude soupçonnée ou avérée ?
Comprendre, traiter, remédier, améliorer.
Etablir un dispositif de traitement, ce qui veut dire des investigations, des preuves, de la communication interne et externe. On s'aperçoit que, dans les cas de fraude, ce qui disparaît le plus rapidement, ce sont les preuves. Si l'on met un certain temps à réagir, les preuves auront disparu et il sera très difficile ensuite de reconstituer les opérations.
Gérer les cas de fraude détectés. Cela n'est pas facile, et peut ensuite générer des pertes, une problématique de réputation pour l'entreprise, une problématique d'image.
Appliquer les sanctions prévues par l'entreprise.
Adapter et améliorer le dispositif de prévention, avec une autoévaluation des risques de fraude.
C'est ce dispositif que l'on est en train de mettre en place à Groupama Banque, en capitalisant sur nos expériences passées et pour améliorer notre future organisation.

Marc FOURRIER

Notre approche est tout à fait similaire.

J'insisterai sur le préalable à la construction d'un programme de ce type qui est d'avoir entrepris une démarche éthique au sein de l'entreprise, d'avoir bien cadré tout ce qui concerne la déontologie, et d'avoir formé le personnel aux valeurs de l'entreprise, et à ce qu'il faut faire ou ne pas faire.
Le programme n'est pas un programme caché. Il fait partie de la communication. Il faut que tout le monde, dans l'entreprise, sache que la fraude, ce n'est pas attraper le fraudeur et le mettre à la porte, c'est avoir une démarche concrète et structurée qui s'intègre dans un processus global de contrôle interne.

Nous avons initié cette approche en 2006 sur la partie de la prévention qui concerne la sensibilisation des salariés. Cela nous a paru extrêmement important. Il faut se souvenir qu'en 2006, on ne parlait pas de la fraude interne comme on en parle aujourd'hui ; il n'y avait pas eu Madoff, il n'y avait pas eu Kerviel. Nous étions encore dans une zone taboue.

Quand nous avons commencé à parler de la mise en place d'un dispositif antifraude, nous avons enregistré un certain nombre de réactions qui nous ont amenées à aborder le sujet de façon très concrète. Pour ma part, dans une démarche un peu marketing, j'ai suggéré des *focus groups*, des tables rondes avec les salariés de l'entreprise pour comprendre leur perception sur ce sujet dont on ne parlait pas.
En parallèle, nous avons travaillé sur les typologies de fraude, pas d'un point de vue technique, mais mieux comprendre où étaient traités ces types de risque dans l'organisation et quels étaient ceux qui

allaient être pris en compte par la coordination de la lutte anti-fraude, ce qui n'est pas un sujet très facile.
Cela nous a amenés à définir pour l'entreprise, ce qu'est le risque de fraude interne, avec les termes appropriés, compréhensibles par tous les collaborateurs de l'entreprise, les mandataires, les agents généraux distributeurs. Et nous avons entrepris une première cartographie des risques de fraude pour savoir où se logeaient les risques.
Nous avons construit une charte anti-fraude qui expose aux salariés la politique de la compagnie en matière de fraude et leurs obligations face aux risques de la fraude. Il faut se souvenir que nous exerçons des activités de services, donc très dématérialisées, et que nous n'existons que si le client a confiance en nous. Toute notre argumentation et toute notre communication ont donc porté sur le risque de rupture de confiance avec les clients, notamment si l'on est dans des zones de risques de fraude. Cette charte, associée au code de déontologie, est remise à tous les nouveaux entrants ; elle fait partie de la formation des salariés.
Dans une grosse organisation, il faut des relais. La coordination de la lutte anti-fraude est une fonction centrale et, fonctionnellement, s'appuie sur un réseau de correspondants anti-fraude qui a été créé au sein des directions de contrôle permanent, et maintenant des responsables *compliance* au sein de l'organisation.

Nous avons construit un programme de sensibilisation destiné à tous les salariés, en trois étapes.
La première étape a consisté à vendre le projet à la direction générale, qui en est devenue le sponsor. C'est un point essentiel. Le PDG est intervenu dans le programme de sensibilisation destiné aux soixante quinze dirigeants de l'entreprise.
La deuxième étape concernait les 1600 managers. L'accent a été mis sur les responsabilités liées à leur fonction, sur la maîtrise du risque de fraude et le devoir de vigilance. Exemplarité pour les dirigeants, vigilance pour les managers.
La troisième étape a été la diffusion d'un programme de sensibilisation, via l'intranet, à l'ensemble des salariés du groupe Cela s'est traduit par des conférences sur site – site de gestion, fonction centrale, etc. – pour sensibiliser au risque de fraude, au risque de rupture de confiance et aux conséquences du risque de fraude.
En parallèle, des travaux très concrets (parce que la sensibilisation peut paraître quelque peu évanescente) ont été menés sur l'élaboration de la cartographie des risques de fraude : brainstormings, réflexions, travaux sur l'identification des risques, avec l'élaboration d'une méthodologie systématique, par processus. Nous avons associé ces travaux à une campagne d'affichage interne dans cinquante sites de l'entreprise en France et à des conférences internes. Nous avons d'ailleurs continué cette campagne par une campagne sur d'autres natures de risques (sécurité informatique, blanchiment, etc.) qui peuvent y être associés. Le sujet de la fraude est traité régulièrement en Comités de Contrôle Interne et l'état du programme anti-fraude présenté annuellement au comité exécutif. Un rapport annuel est publié chaque année et présenté au comité d'audit et au conseil d'administration, avec les résultats et l'évaluation du dispositif par l'audit.

Au bout de trois ans, nous avons acquis beaucoup plus de maturité. La communication régulière sur le sujet de la fraude est tout à fait acceptée. Notre cadre de contrôle interne est beaucoup plus construit, ce qui permet de l'intégrer plus facilement.
Aujourd'hui on a tué le tabou, je pense ; on peut parler librement de la fraude, en prenant quelques précautions. Les messages sont plus directs. Les opérationnels souhaitent pouvoir communiquer de façon beaucoup plus concrète sur différents cas. C'est à la fois très bien et très délicat. Le problème est évidemment de ne pas dévoiler certaines choses et de ne pas donner à tout le monde un « livre de bonnes recettes pour frauder ». On organise donc des petits groupes de travail extrêmement ciblés, qui permettent de faire des analyses post-mortem de cas, et d'en tirer des conclusions pour améliorer nos systèmes d'information.
Voici quelques conseils tirés de mon expérience. Attention à la sémantique ! Les cultures d'entreprise sont diverses ; elles sont propres à chacun. Il y a des mots ou plutôt des raccourcis qui peuvent fâcher : la surveillance, par exemple. Alors, on ne parlera pas de surveillance, mais de prévention ;

détection proactive fait un peu chasse au fraudeur, on parlera de détection d'anomalies susceptibles de révéler des fraudes, etc. Concrètement, cela ne change pas la façon opérationnelle dont on traite les affaires, mais cela facilite la communication. Cela permet de parler du programme, et de donner les résultats, les enseignements qui en découlent, et bien sûr de stigmatiser les faits et non les personnes. Nous veillons particulièrement au respect de la loi Informatique et Libertés.

Philippe GREAT

Je vais vous parler des premières étapes de la mise en œuvre du dispositif de prévention de la fraude.

En premier lieu, vient **l'identification et l'évaluation** des principaux domaines de risques, les facteurs d'exposition et les axes d'analyse : les défaillances constatées (que s'est-il passé et que faut-il faire pour éviter que cela se reproduise ?) ; les indicateurs ; les niveaux d'exposition ; les degrés de maîtrise permettant de mettre au point une cartographie ciblée des risques de fraude en fonction des différentes activités.

Ensuite, **expliquer**, encore et toujours, les enjeux et l'importance du dispositif de contrôle à l'ensemble des intervenants internes et externes. Définir un « qui fait quoi ». Communiquer sur le risque de fraude, expliquer qu'une fraude, cela peut arriver, que cela peut toucher n'importe qui, à n'importe quel moment, n'importe quelle organisation, organisation préalablement touchée ou pas. On constate que certaines organisations s'estiment être non concernées par le problème de la fraude, ce qui est totalement irréaliste.

Développer et promouvoir une culture d'éthique et de déontologie, avec un règlement intérieur, des règles de comportement et de bonne conduite applicables à tous ; une politique RH : chaque fois qu'un nouveau collaborateur entre dans l'entreprise, on lui fait prendre connaissance de ces éléments. On lui fera suivre – on y reviendra tout à l'heure – des formations, de même d'ailleurs qu'à tous les collaborateurs. Il faudra définir nos mandats d'intermédiaire en opérations bancaires, puisque nos produits sont commercialisés par le réseau dans le Groupama Gan.

Définir une politique interne de responsabilisation et de contrôle. Il s'agit là des règles de délégation – n'importe qui ne peut pas faire n'importe quoi à n'importe quel moment –, de responsabilité, de reporting ; bien préciser le rôle des différents acteurs et des intervenants ; définir des consignes de sécurité, avec des approbations préalables ; définir un environnement de contrôle, des procédures, etc. Cet ensemble d'éléments doit nous permettre de réduire la fraude autant que faire se peut.

Sensibiliser et former, de manière permanente et adaptée, les collaborateurs : c'est un chantier en cours, que l'on va continuer de développer en fonction des différents métiers et des collaborateurs. Chaque collaborateur ne traitant pas les mêmes matières, n'est pas concerné par un même risque de fraude. Formations présentielles, *e-learnings*, échanges avec les collaborateurs et les managers, communication sur la politique générale et sur les règles internes, veille réglementaire, mise à disposition d'informations utiles et pertinentes permettant de reconnaître une opération frauduleuse, responsabilisation des collaborateurs à tous niveaux et à tous échelons, communications sur les risques et les sanctions.

Mettre en place un système d'alerte et de prévention basé sur des outils : ce n'est pas nouveau, mais nous sommes partis de là et je pense que cela a tout son sens ; des outils de « direction » ; ce sont les règlements, codes, procédures, signatures, habilitations, etc. Des outils de « permission » : contrôles d'accès physique et logique, séparation des tâches, délégations… Des outils de « détection » : systèmes d'alerte, collecte des incidents (il est très important de mettre en place, dans une

entreprise, des remontées d'incidents, car cela permet d'inciter les collaborateurs, de les impliquer dans la démarche, même si l'on reçoit parfois des informations qui ne sont pas vraiment des fraudes ni vraiment des incidents, j'en conviens. Mais ce n'est pas grave, l'idée est que chacun puisse faire remonter, à sa manière, les éléments importants, et se sente acteur du dispositif), inventaires, confirmations, circularisations, enregistrement des transactions, contrôles a priori, préventifs, et a posteriori, comptes rendus, etc.
Piloter et coordonner de manière centralisée la mise en œuvre du suivi et du contrôle du dispositif : cela nous est venu de nos expériences passées. Nous nous sommes rendu compte que mettre en place un dispositif centralisé permettait de mieux gérer le dispositif que d'avoir des dispositifs de contrôle épars dans toutes les institutions.
Cela ne veut pas dire que je fais tout, cela veut dire que tout est centralisé, en ce qui concerne le pilotage, à un seul et même endroit. Ce sera une veille stratégique, une appréciation constante de l'environnement et de son évolution, un suivi des indicateurs et un examen des facteurs favorisant la fraude, etc.

Marc FOURRIER

Pour enchaîner, nous allons parler de programmes et de contenus et des acteurs de la prévention, qui sont en général les acteurs de l'ensemble du programme.

Chez Allianz, il y a un chef d'orchestre, le **coordonnateur de la lutte antifraude (CLAF)**, qui séquence et organise le programme pour l'ensemble du groupe France ; met en place les protocoles transverses nécessaires (prévention, évaluation des risques, détection, protocole d'investigation, etc.) ; anime son réseau de correspondants ; coordonne les actions de prévention et fournit du matériel pour la démultiplication, dans toutes les entités ; collabore étroitement avec les fonctions liées au risque et au contrôle interne que sont l'audit, le *risk management* et le contrôle permanent.

Le **réseau de correspondants anti fraude**. Ce sont en général les *compliance officers* ou les contrôleurs permanents, très sensibilisés aux risques, qui animent les structures locales.

Une **direction des risques et du contrôle permanent**. Dans le cadre de l'évaluation des risques, toutes les cartographies s'insèrent dans une cartographie globale des risques de la maison, laquelle donne lieu à une communication.

La **direction de l'audit** évalue annuellement le dispositif anti fraude de la direction de la conformité ; alimente la capacité à mieux maîtriser les risques de fraude par les résultats des missions et les recommandations formulées ; effectue, chaque année, sur demande ou de son propre chef, un certain nombre de missions spécifiques sur la fraude : cela peut être soit des évaluations détaillées de telle ou telle partie d'un dispositif dans tel ou tel secteur, soit une analyse post-mortem sur un certain nombre de cas ou sur un cas donné, sur le déroulement, le mode de détection, le mode de traitement.

Des **fonctions « partenaires »** clés : RH, RSSI, Comptabilité, Trésorerie, etc.

Des **instances régulièrement informées** : le comité de contrôle interne, le comité d'audit, etc.

Le **réseau international groupe**, source de partage des meilleures pratiques.

Philippe GREAT

Dans une organisation, tout le monde est concerné par la vigilance en matière de lutte contre la fraude, qu'elle soit interne ou externe. Il existe un dispositif, piloté par la sécurité financière. Mais elle ne pourra pas le faire seule, ni sans la volonté de la direction générale.

Quels sont les intervenants ?

L'inspection audit, partie prenante du dispositif de fraude, lors de ses missions périodiques.
Les fonctions risques, pour évaluer les risques, vérifier les impacts de la fraude.
La conformité garante des textes et du respect des procédures.
Les RH, qui, dans le domaine du recrutement, sont totalement impliquées dans le dispositif de fraude, et doivent pouvoir cibler les recrutements en fonction des postes et des fonctions.
Les fonctions de contrôle permanent qui, lors de leurs contrôles sur place et sur pièces, effectuent des vérifications, font remonter des informations, et sont à même de détecter des cas de fraude.
Les collaborateurs et les managers, puisque toutes les fonctions opérationnelles de Groupama Banque sont concernées, mais pas uniquement elles.
Les fonctions support – finances, affaires juridiques, réclamations, et j'en passe – qui peuvent, elles aussi, faire des constats. Les réclamations des clients, par exemple, sont souvent des vecteurs importants de détection d'une fraude.
Le réseau commercial peut faire remonter des alertes.
Les responsables conformité et contrôle interne peuvent faire remonter des éléments d'alerte sur des fraudes internes ou externes.

Si l'on résume les fonctions de contrôle interne, on trouve les contrôles permanents de premier niveau (contrôles opérationnels…) ; les contrôles permanents de deuxième niveau (spécifiques à la banque : appréciation de la cohérence et de l'efficacité des contrôles de premier niveau) ; les contrôles périodiques de troisième niveau assurés par l'inspection. Tous ces acteurs doivent être sensibilisés et informés sur l'ensemble des cas de fraude.

Le rôle de la sécurité financière est de coordonner et de piloter l'ensemble de ce dispositif, et d'en assurer la cohérence.

Marc FOURRIER

Est-il utile de préciser que la fraude est un défi permanent ? Il est donc indispensable d'évoluer constamment. Des facteurs aggravants – la crise économique, la réorganisation des entreprises, la mobilité du personnel, etc. – accroissent la vulnérabilité, surtout si les contrôles ne sont pas à la hauteur. Face à l'esprit d'innovation des fraudeurs, il faut essayer de conserver un cran d'avance. Pour cela, il est nécessaire de sensibiliser régulièrement les opérationnels et tous les acteurs en général.
Les conditions de succès d'une bonne sensibilisation sont au nombre de sept.

Philippe GREAT

La première condition est **l'implication visible de la direction générale**.

Marc FOURRIER

Visible, et ce n'est pas qu'une façade. Visible, touche au risque pénal et au risque d'image ; le dirigeant est extrêmement sensible à cela.

Une démarche éthique bien ancrée. Il est en effet important d'avoir démarré sur la base d'une démarche éthique/déontologie, pour pouvoir construire un programme efficace.

Une bonne connaissance des risques de fraude, cela va de soi. On sait de quoi on parle et il est vrai que, lorsque l'on a un peu plus d'expérience dans la démarche, on peut illustrer très concrètement le phénomène et les risques pour l'entreprise.

Philippe GREAT

Sensibiliser sans tabou, c'est-à-dire qu'il faut être capable de parler, de la manière la plus libre qui soit, de la fraude. C'est un sujet capital qui joue sur l'existence de l'entreprise, qui joue sur nos métiers. Chacun, à son niveau, doit prendre conscience de ses responsabilités et des risques qu'il fait encourir à l'entreprise lors d'une fraude.

Marc FOURRIER

Exploiter, dans le cadre d'un programme structuré, **toute action anti fraude** sous l'angle d'une communication positive. Communiquer sur le programme : je l'ai déjà dit, ce n'est pas un programme caché, c'est un programme ouvert. On peut l'inscrire dans une approche de contrôle interne, dans une approche éthique, mais on essaie de faire cette synthèse et, dès lors qu'il y a des pans, des blocs d'activité qui sont lancés ou un programme particulier ou des priorités annuelles, on communique le plus largement possible, en rendant le sujet de la fraude aussi concret que possible. Il ne s'agit pas de dénoncer des personnes, mais de mettre en place un véritable programme de maîtrise des risques.

Utiliser le réseau : il faut avoir ce réseau, ou bien le construire. Dans une grosse organisation, on ne peut pas se passer de ces réseaux qui seront le relais de la démultiplication. Ils seront moteur pour le référencement des cas, le reporting, la détection proactive d'anomalies, le traitement des cas. Ils seront la cheville ouvrière au sein des unités, des groupes opérationnels qui, chez nous, sont dotés de structures de contrôle permanent, et notamment de conformité.

Philippe GREAT

Maintenir une veille stratégique permanente. Pourquoi ? Pour apprécier, de manière constante, l'environnement, puisque, je l'ai dit tout à l'heure, si l'on ne fait rien, si on laisse les choses en l'état, on se laisse déborder : l'environnement d'aujourd'hui n'est pas l'environnement de demain. Il faut donc être capable d'évoluer en permanence.

Cela va permettre de détecter les signaux d'une fraude pouvant affecter la stratégie de la banque, pour nous, ou de l'organisation en général ; d'examiner les facteurs favorisant la fraude à un instant « T », qui peuvent être différents demain, pour diverses raisons : réorganisation d'un service, fusion, etc. ; de suivre des indicateurs, de les mettre à niveau, bref, de disposer d'un support complet de l'organisation.

Ces sept points nous paraissent essentiels dans un dispositif de sensibilisation et de prévention de la fraude.

Jean-François SAUTIN

En cas de suspicion de fraude, vous dites qu'il faut agir vite et bien.

Mais, bien souvent, dans nos organisations, les gens ne savent pas comment agir. Ils peuvent faire un faux pas et faire disparaître des preuves, ou créer des problèmes de gestion des ressources humaines en incriminant malencontreusement certaines personnes.

Comment, dans vos organisations, traitez-vous de cette problématique ? Existe-t-il des formations spécifiques pour aider les gens à avoir les bons réflexes quand se présente un cas de suspicion de fraude ?

Marc FOURRIER

Cela n'a pas été notre premier chantier. On était alors dans un mode réactif : on découvrait une fraude, on traitait. Après avoir mis en place des programmes de prévention et de détection, on s'est rendu compte qu'il fallait faire les choses en profondeur dans ce domaine, d'autant que le groupe avait été réorganisé de façon matricielle, et que la question du « qui fait quoi » se posait d'une façon nouvelle.

Un chantier, qui a bien duré une année, a consisté à formuler un protocole d'investigation : qui fait quoi, quand il y a soupçon de fraude et quand la fraude est avérée ? Qui intègre la partie « récolte des preuves » et le travail avec les acteurs clés dont j'ai parlé, notamment la RH, le RSSI.

Nous avons essayé – et ce n'est pas simple – de formaliser tout cela, sachant que nous ne disposons pas d'une équipe polyvalente d'investigateurs. L'audit a donc là un rôle important à jouer, comme je l'ai signalé, en matière d'investigation notamment.

Philippe GREAT

Chez Groupama Banque, c'est la même chose, c'est-à-dire qu'il faut être capable de prévoir des scénarios et les anticiper. C'est un peu comme dans l'aviation : même s'il y a très peu de risques qu'un crash se produise, il faut prévoir la communication dans le cas où il surviendrait.

Selon l'importance de la fraude détectée ou de la fraude communiquée, il faut être à même de prévoir des scénarios de réponse, il faut être capable d'anticiper. Tous les acteurs concernés – au premier rang desquels l'audit et l'inspection, bien évidemment – ont un rôle majeur pour tout ce qui concerne les entités du groupe.

QUESTIONS/REPONSES

Question

Concernant cette volonté de communication ouverte et sans tabou, dont vous avez parlé, comment placez-vous le curseur entre cette attitude et une certaine nécessité de confidentialité à l'égard d'une fraude qui signifie forcément une défaillance dans l'entreprise ?

Philippe GREAT

On peut communiquer sans tabou sur des cas généraux, sur des cas qui se sont déjà produits, puisqu'ils sont connus. La communication doit être évidemment beaucoup plus ciblée sur les enquêtes et les cas en cours, ou sur les cas avérés en cours de détection.

Il y a deux cas de figure. Il faut d'une part être capable de répondre lorsqu'un événement se produit, et il faut d'autre part pouvoir communiquer sans tabou de manière générale sur la fraude, en expliquant à l'ensemble des collaborateurs comment fonctionne le dispositif, comment y faire face et éviter les risques.

Marc FOURRIER

J'évoquais le fait que nous sommes de plus en plus amenés à communiquer, auprès des opérationnels, sur des cas de fraude très concrets. C'est évidemment anonymisé ; nous avons la chance d'avoir un certain nombre d'entités, ce qui permet d'utiliser les cas d'une filière d'une autre entité pour en parler de façon anonyme, mais très technique, très factuelle. C'est plein d'enseignements.

Il ne faut évidemment pas aller trop loin, et « donner des moyens de frauder mieux », mais, à ce stade, cela ne pose pas de problème particulier. On ne parle évidemment pas des personnes ; on évoque des faits, des failles dans les systèmes d'information, etc.

Question

Disposez-vous d'une mesure ou d'une évaluation de l'efficacité ou de l'efficience de ce dispositif ?

Philippe GREAT

Si l'on met en place un dispositif, c'est bien pour mesurer son efficacité, vérifier s'il fonctionne et s'il a une valeur ajoutée. Sinon, cela ne sert à rien de le mettre en place. Il faut donc prévoir des indicateurs de mesure. Cela veut dire aussi qu'il faut être capable de se remettre en question quand on s'aperçoit que les mesures mises en place ne fonctionnent pas ou ne donnent pas les résultats attendus, et évoluer en permanence.

Marc FOURRIER

Nous sommes évalués tous les ans par l'audit, selon une méthodologie bien établie ; il y a une part qualitatif et une part quantitatif. Nous sommes d'abord dans un dispositif de type conformité avec un objectif d'*operative effectiveness* pour la mesure de l'ensemble du dispositif : a-t-on utilisé les bons moyens en termes de prévention, en termes de détection ?

Après, on peut regarder les résultats, et on est plus dans un mode quanti où, quand on dispose d'une base de données – comme c'est le cas maintenant, après plusieurs années et des centaines de cas –, on peut mesurer un peu mieux l'évolution en matière de taux de détection, de délais de détection des cas, de taux de recouvrement, etc.

Nous disposons de toute une batterie d'indicateurs qui permettent de voir dans le temps – c'est du moyen terme, ce ne sont pas des choses que l'on peut mesurer à court terme –, d'essayer de mesurer l'efficacité du dispositif. Mais sur des sujets comme la sensibilisation ou même l'évaluation de la cartographie des risques de fraude, nous sommes plus dans du qualitatif : a-t-on employé les bons moyens, tout cela s'insère-t-il bien dans un ensemble, notamment l'ensemble des contrôles internes pour la cartographie ?

Noël PONS

Lorsque vous avez mis en place ces systèmes, avez-vous rencontré des points particuliers de blocage, ou des éléments ont-ils fait que, à un moment, vous vous êtes dit qu'il y avait un problème ? Et dans quel(s) domaine(s), s'il vous est possible d'en parler ?

Marc FOURRIER

Le démarrage sur les mots employés n'a pas été simple. On a peut-être pris des fausses pistes, puis on a rectifié le tir. Je vous ai parlé de l'importance de l'environnement culturel et des mots à éviter.

Autre sujet : le dispositif d'alerte éthique était, à une époque, un élément bloquant. Cela l'est beaucoup moins aujourd'hui, parce que la CNIL a pris une position beaucoup plus claire sur le sujet.

Il y a eu en effet quelques blocages, mais ils n'ont pas remis en cause la politique que nous avions publiée, et tout le monde était d'accord sur le fait qu'il fallait maîtriser le risque de fraude, tout en faisant très attention à la façon d'en parler.

Philippe GREAT

J'ajouterai que, dans la mise en œuvre, la difficulté est de faire passer le message que « cela n'arrive pas qu'aux autres », de faire prendre conscience à chacun des enjeux, à tous les niveaux.

Une autre difficulté que l'on rencontre est d'impliquer chacun des acteurs et de trouver une solution pour l'impliquer ; elle ne sera pas la même pour tous : commerciaux, services opérationnels, RH, etc. Il n'est pas simple de s'adapter à la problématique et au langage dans des entités qui traitent une grande variété de sujets.

Vianney DUMONT, audit interne MAIF

Ma question porte sur la politique de coordination de la lutte antifraude. Chez Allianz, il y a un coordonnateur de la lutte antifraude, au sein de la fonction conformité. Faut-il comprendre que chaque métier, ou les principaux métiers – Sinistres, Contrats, Finances, Informatique, etc. – ont leur propre fonction antifraude coordonnée du point de vue des méthodes, etc., par la fonction conformité ? Et y a-t-il une dépendance fonctionnelle, dans ce cadre-là, des fonctions antifraudes métiers à la coordination centrale ?

Marc FOURRIER

J'ai signalé en préambule que la coordination de la lutte antifraude se concentrait sur la fraude interne. Pour la fraude externe qui est très opérationnelle, la responsabilité est entièrement au sein des lignes de métier.
Il existe en effet un rôle fonctionnel, un rôle d'animation, au sein des unités opérationnelles, des lignes de métier, – je prends cet exemple-là, mais il y a la même chose pour la distribution et les différents réseaux de distribution – avec un coordonnateur « local » (ce n'est pas péjoratif) de ces unités, qui est en fait le relais fonctionnel de la coordination anti-fraude et qui l'assure, au sein de son organisation.
Cela a pris quelques mois pour être mis en place, et en se posant la question de la légitimité de ce réseau. Mais aujourd'hui, le principe est bien établi ; cela fait partie des fonctions, notamment des fonctions de contrôle. Ce n'est donc pas un poste « à part ».
Sur les grosses entités, la *compliance* est un poste à part entière, et la fraude fait partie d'un ensemble maintenant bien unifié en termes de conformité.

Vianney DUMONT

Cela signifie-t-il que le travail opérationnel de détection de fraudes internes, comme par exemple le balayage systématique des mouvements informatiques, est fait au niveau des métiers ?

Marc FOURRIER

Il y a deux niveaux. Pour simplifier, les contrôles des différents processus intègrent en effet des contrôles détectifs. Il ne s'agit donc pas de refaire le travail que font les opérationnels en matière de contrôle. En revanche, nous avons, plutôt en central, les correspondants qui pilotent un chantier détection de scénarios donnés, qui ne sont pas nécessairement des scénarios de fraude, et qui sont intégrés ou spécifiquement répertoriés dans les contrôles des processus ; également en central, une personne fait de l'analyse de données. Cela fonctionne en collaboration, en co-pilotage avec les directions concernées.

Il ne s'agit pas de se substituer au contrôle permanent, mais d'accentuer la recherche dans des domaines que l'on pense ne pas avoir suffisamment explorés.
Ensuite, cela peut en effet devenir un processus régulier qui se réintègre dans le contrôle permanent, avec un outil spécifique.

Philippe GREAT

Pour nous qui avons a une démarche centralisée, la chose, au moins sur le papier, est plus simple : nous récupérons les données de l'ensemble des intervenants, construisons nos propres indicateurs et recueillons nos propres données. L'idée est d'avoir une vision totalement cohérente et de piloter l'ensemble. Si l'on n'a jamais vérifié la source de ces données et leur qualité, on peut douter de leur efficacité. Il faut donc être capable, lorsque des données nous sont remontées, de s'assurer qu'elles sont conformes et correctes. On va pour cela s'appuyer sur le dispositif de contrôle permanent.

Question

Pour avoir été acteur d'actions d'objectivation de fraude – en audit interne, on nous envoie sur des fraudes suspectées que l'on doit objectiver techniquement, puis faire avouer le fraudeur – je peux dire que cela n'est pas simple. On a dit tout à l'heure que les fraudeurs ont énormément d'astuce pour inventer, pour innover dans la fraude. En général, et pour les mêmes raisons d'agilité psychologique, ils ont aussi beaucoup d'astuce pour botter en touche, pour faire l'anguille, pour expliquer que ce n'est pas eux, que c'est l'autre, expliquer je ne sais quoi.
Il y a aussi le rôle du manager (cela surprend au début et puis on finit presque par le comprendre), souvent protecteur, expliquant, justifiant, et ce d'autant plus qu'il n'est pas toujours très « net » dans l'affaire.
Dans le rôle d'objectivation, il y a surtout le très gros risque de briser quelqu'un, et l'on s'interdit – en tout cas, je me l'interdis et je pense que tout auditeur se l'interdit – de prendre ne serait-ce que 1 % de risque de commettre une erreur judiciaire.
Et l'on s'aperçoit finalement que, malgré notre intime conviction, malgré notre certitude absolue, rien n'est absolument certain, rien n'est tout blanc ou tout noir, mais le plus souvent gris, voire gris foncé, et c'est un peu frustrant.

Vivez-vous cela ? Comment le gérez-vous ? Formez-vous des gens aux techniques d'inspecteurs chevronnés ?

Marc FOURRIER

Vous avez raison, ce n'est pas simple. On aura beau écrire les meilleurs protocoles d'investigation de la terre, on sera toujours dans du cas par cas.

Une fois recueillies un maximum de preuves, une fois menés des entretiens conjoints, il peut malgré tout manquer un élément probant. Et à un moment donné, une décision doit être prise : on sanctionne ou on ne sanctionne pas ? Dans tous les cas, il y a une prise de risque.

Philippe GREAT

Cela me paraît évident. Et la difficulté est de distinguer l'erreur de la fraude ? Est-ce une erreur de saisie ou un acte de malveillance ? Il y a bien sûr des indices : phénomènes répétitifs, montants astronomiques…
L'audit n'est pas là pour se substituer à des services de police, ou à des magistrats. Une fois découverte une fraude avérée, l'audit doit passer le relais. Le rôle de l'audit est de protéger les

intérêts de l'entreprise, et de faire en sorte que la fraude soit arrêtée, et que des solutions soient trouvées pour qu'elle ne puisse pas se renouveler.

Jean-François SAUTIN

Nous poursuivons avec une présentation de Sébastien Allaire et Beatriz Sanz Redrado sur le thème « Comment construire une cartographie des risques liés à la fraude ? »

Beatriz Sanz Redrado a récemment pris la responsabilité de l'audit interne du Groupe Galeries Lafayette.

Sébastien Allaire est associé au sein de la ligne de services *Risk management*, audit interne et contrôle, chez Deloitte Conseil.

COMMENT CONSTRUIRE UNE CARTOGRAPHIE DES RISQUES LIES A LA FRAUDE ?

Sébastien ALLAIRE, *Associé, Deloitte*

Beatriz SANZ REDRADO, *Directeur Audit, Groupe Galeries Lafayette*

Sébastien ALLAIRE, *Associé, Deloitte*

Nous allons parler d'un sujet assez pointu, novateur, obscur pour certains, qui est la cartographie spécifique des risques de fraude. Nous allons faire une présentation à la fois un peu théorique (le point de vue d'un cabinet), et pratique, avec des expériences et des exemples concrets.

Pourquoi une cartographie spécifique du risque de fraude ? C'est la première question que l'on s'est posée. Aujourd'hui, le cadre réglementaire impose aux groupes cotés d'établir une cartographie globale des risques.
Cette cartographie identifie pour le management les principaux risques – que l'on appelle le « top 20 » ou le « top 10 » – censés être, selon les approches *top down* ou *bottom up*, une agrégation par paniers, ou de manière plus scientifique par modélisation, des risques majeurs, ou, selon une perception plus empirique du top management, de ce qui est critique pour l'entreprise.
On observe d'ailleurs, avant 2008, que ces cartographies des risques mentionnent assez rarement le risque de fraude en tant que tel. La fraude « peut exister ». Elle existe de fait dans toutes les entreprises. Le risque de fraude est un risque inhérent à toutes les organisations. C'est un risque qui peut avoir des impacts financiers non négligeables, et des impacts sur l'image. A ce titre, il doit figurer sur la cartographie des risques, dans la liste des risques majeurs suivis par le top management. Il doit être cartographié de manière spécifique.

Quel univers pour analyser le risque de fraude ? Il existe plusieurs typologies de fraude. Les normes d'audit américaines et internationales, déterminent deux grandes natures de fraude : le détournement d'actifs, immatériels ou matériels, et la manipulation des indicateurs de performance et des états financiers. A cela, on rajoute communément, peut-être par souci de simplification, une troisième catégorie qui est la corruption, active ou passive. On trouve des typologies plus détaillées, mais on se limite, en cabinet, à une typologie relativement succincte.
Une fois identifiées les trois grandes natures de fraude, dans quel domaine cette fraude peut-elle s'appliquer? On se reporte là à l'approche – peut-être la plus communément utilisée aujourd'hui par les entreprises – de *risk management* américaine COSO 2 ou ERM, et qui découpe l'entreprise en quatre grandes natures d'opérations : les risques stratégiques, les risques opérationnels, les risques comptables et financiers et les risques liés à la conformité réglementaire. La fraude, selon la typologie, peut se retrouver dans l'un de ces quatre piliers. Il ne faut pas oublier la dimension informatique transversale à l'organisation, et qui, en soi, représente un risque important, ou en tout cas une source potentielle de fraudes.

Quelle démarche déployer pour cartographier les risques ? Il peut y avoir débat entre le *top down* et le *bottom up*.
Avant de donner la conclusion, on observe aujourd'hui, dans les dispositifs de lutte contre la fraude, trois étapes, qui sont peut-être liées à la maturité de l'entreprise.
La première étape est la sensibilisation, la responsabilisation. Elle se traduit par les chartes ou les codes d'éthique, les formations, la communication interne… Cela ne protège pas contre la fraude, ne permet pas de détecter les fraudes, mais, en renforçant l'éthique, peut réduire le risque de fraude.
La deuxième étape est d'écouter. Les systèmes d'alerte, *hotlines*, *whistleblowing*, plus ou moins déployés selon les réglementations, permettent au management de prendre connaissance des cas de fraude. La limite du système, là encore, est que tout ce qui n'est pas communiqué au management n'est pas censé exister. D'où la difficulté pour le management d'appréhender et d'anticiper le niveau d'exposition au risque de fraude.

La troisième étape est la cartographie.
Nous, Deloitte, recommandons de commencer par l'approche *top down*. La fraude est transverse et polymorphe, tout le monde le sait, et cela s'applique à tous les niveaux de l'entreprise. Donc, une approche *bottom up* globale, qui envoie à toutes les personnes de l'entreprise des questions sur la fraude, risque d'être compliquée, et génère des volumes très élevés de risques identifiés, d'incidents ou autres ; et ensuite, il faut remonter du terrain jusqu'au top management pour identifier les actions prioritaires des risques les plus forts. L'exercice de remontée et d'agrégation est relativement compliqué.
Sensibiliser l'ensemble de l'organisation, soit ; mais questionner l'ensemble de l'organisation sur ce que l'on pourrait faire pour contourner les systèmes, contourner les contrôles et frauder, c'est finalement un peu donner le bâton pour se faire battre ; c'est demander à tout le monde de réfléchir sur comment faire mal les choses, ce qui peut avoir des conséquences qui ne sont pas forcément celles que l'on souhaite.

On en vient donc à une approche par le haut, qui est de se dire : commençons par se poser les questions.
Où sommes-nous exposés à la fraude du fait de notre activité, du fait de la localisation de nos activités, du fait de la nature de nos produits ? Et, une fois que l'on a commencé à identifier les sujets qui nous semblent prioritaires en termes d'analyse – on n'a pas encore la réponse –, descendons à ce moment-là sur ces sujets au niveau du terrain, de manière ciblée (donc sur du *top down* ciblé) pour demander à quelques interlocuteurs sélectionnés, quelques opérationnels sélectionnés, leur perception, leur connaissance, leur vision du risque de fraude à leur niveau.
On part d'une identification des risques majeurs, par des ateliers de travail. Puis on décline des risques majeurs en risques individuels. Un risque majeur est une sorte d'arbre, dont les branches sont autant de conséquences possibles, et les racines les causes possibles. L'idée est de descendre dans l'organisation pour analyser les racines propres à l'arbre que l'on aura sélectionné. Une fois que l'on est au niveau des racines, donc opérationnel, on apprécie l'exposition de chaque racine au risque, avec le management des entités.
Il y a – c'est une particularité que l'on va vous présenter – une démarche sélective, par tests, des schémas de fraude, avec l'appui d'experts. Dès lors, deux questions se posent. Une première question sur l'indépendance : demander à un opérationnel si tel schéma de fraude peut fonctionner chez lui, c'est en quelque sorte lui donner les clés du schéma de fraude et cela devient quelque peu dangereux. Une deuxième question sur la compétence : enquêter sur une fraude requiert des techniques, des réflexes, une sensibilité juridique qui n'est pas forcément dans la mallette de tout auditeur interne : il y a, là encore, un besoin d'anticiper des démarches un peu spécifiques.
Une fois ce travail fait, on remonte au niveau de l'arbre. On connaît un peu l'état des racines et on est capable de donner une évaluation d'un arbre par rapport à un autre, l'état des lieux, et les plans d'action qui en découlent.

Prenons par exemple, dans la typologie des risques, le détournement d'actifs. Les risques majeurs se classent en deux catégories : les détournements de biens matériels et de biens immatériels. Dans le secteur industriel, les biens matériels peuvent être des stocks, des immobilisations corporelles, du cash, etc.
Ces risques majeurs vont ensuite se décliner en risques individuels. Si je reprends l'exemple des détournements de biens matériels stocks, les risques sont liés à la mise au rebut, aux pièces détachées, aux stocks déportés. J'ai, dans mon réseau, trois entrepôts qui gèrent les stocks de pièces : un qui en gère très peu, et dont je considère que c'est non significatif et je ne l'intègre même pas dans mon périmètre ; deux autres suffisamment significatifs en termes de gestion de pièces détachées pour que je me pose des questions sur le vol de ces pièces.
Je suis là au niveau des racines. Des questions très précises se posent : quelle est la sécurité physique de mes pièces détachées dans les deux derniers entrepôts ? Et selon que mes réponses sont

« bonne » ou « pas bonne », je dois être capable de conclure sur mon vol de stock de pièces détachées qui est une composante, une racine de mon détournement de biens matériels.

Beatriz SANZ REDRADO, *Directeur Audit, Groupe Galeries Lafayette*

Je vais vous parler de la démarche entreprise dans le groupe Galeries Lafayette (GGL) pour identifier les risques majeurs, et élaborer une cartographie des principaux risques, dont celui de la fraude.

Cette démarche, externalisée, a été initiée en 2005, selon une approche *top down*. Nous avons voulu assurer la cohérence des objectifs stratégiques de l'entreprise, qui était l'expansion et l'augmentation du chiffre d'affaires et de la part de marché, en prenant en compte les principaux risques pouvant affecter la réalisation de ces objectifs. Des entretiens ont été menés avec les principaux directeurs et les acteurs de contrôle interne, à l'échelon *corporate* et à l'échelon des branches. Des restitutions ont été faites au niveau du groupe et des entités.

Il y avait des forces et des faiblesses dans cette démarche.
Les forces étaient une vision globale des principaux risques qui pouvaient affecter la société, à un instant T, et une idée très précise des risques majeurs, à surveiller, avec une grande vigilance, dans les différentes activités, qu'elles soient financières, ou de distribution, y compris les risques de fraude qui englobent en fait les risques de vol, de collusion et de fraude pure et dure.
Il y avait aussi des faiblesses : une adhésion tiède, de la part des principaux directeurs qui n'ont pas vraiment été associés à la démarche, mis à part quelques entretiens, et à qui on a présenté le produit fini. Une absence de plans d'actions que masquaient mal quelques suggestions d'amélioration.

En 2008, il y a eu actualisation de la cartographie. Qui dit 2008, dit premiers impacts de la crise financière. Les objectifs stratégiques du groupe, qui étaient la croissance, ont été revus à la baisse. Maintenant, c'est l'amélioration de la marge et la réduction des coûts. Cet objectif modifie la cartographie, en faisant apparaître des risques majeurs nouveaux.
Pour actualiser cette cartographie, on a réalisé l'adéquation entre la stratégie et les principaux risques, et on a procédé par une approche de terrain : depuis 2005, que s'est-il passé ? Des fraudes avérées ont-elles eu lieu ? Des nouveaux systèmes ont-ils été mis en place ?... pour aboutir à la conclusion que la cotation établie sur la base d'entretiens, n'est plus représentative des risques actuels. On a donc modulé ces cotations et l'on a fait ressortir les nouveaux risques, avec des schémas de fraudes identifiées (soit réelles, soit potentielles), par l'audit ou l'inspection.
On s'est rendu compte qu'un des principaux risques encourus était le risque de fraude, et que la fraude est totalement différente selon que l'on parle de Laser Cofinoga ou de Monoprix/GL/BHV ; et qu'elle est également totalement différente, selon que l'on parle d'une fraude commise par les back offices, ou dans les fonctions de vente ou de gestion des stocks. Nous avons donc cartographié en tenant compte de ces critères.
En parallèle, nous avons mis en place des standards pour chaque société, avec un préalable de sécurisation maximum : une stratégie et des objectifs clairement communiqués ; un organigramme fonctionnel ; des fiches de poste ; une séparation des tâches, etc. Nous savons ainsi qui fait quoi, à quel moment, et nous connaissons les responsabilités de chacun.

Sébastien ALLAIRE

Comment évaluer les risques de fraude identifiés ?

La fraude, souvent difficile à appréhender, difficile à évaluer, fait appel à trois facteurs.
L'opportunité : la porte est ouverte, les contrôles ne sont pas en place. C'est un premier critère d'évaluation. Le terrain est plus favorable si portes et fenêtres sont ouvertes ; surtout dans un sous-marin.

La motivation : c'est l'envie de frauder. On est là dans le domaine de l'humain : le besoin d'argent, la crise, les fréquentations. Nous travaillons actuellement sur un cas réel d'une personne qui était a priori intègre, depuis des années dans l'entreprise, et qui, par des évolutions familiales, s'est mise en ménage avec une personne qui, elle, n'avait pas du tout le même niveau d'intégrité et qui l'a conduite à réaliser des fraudes massives dans son entreprise. Cela s'est très mal terminé. La motivation, facteur humain, est très difficile à évaluer.
La rationalisation : « Je fraude, mais ce n'est pas grave, parce que je ne suis pas le seul. » En interne : « Mon copain, mes patrons fraudent, donc moi aussi. Il n'y a pas de raison. De toute façon, ce que je fais, par rapport à mon patron, c'est rien. » En externe : « Les scandales financiers que l'on découvre tous les jours dans la presse me disent que l'on vit dans un monde où l'éthique est très faible ; pourquoi serais-je le seul à être tout de blanc vêtu dans un monde qui ne porte pas cette couleur ? »
Ces trois facteurs vont déterminer l'occurrence de la fraude et sont difficiles à évaluer.

On propose aujourd'hui une approche en deux temps, qui prend en compte les spécificités du risque de fraude, ainsi que la volumétrie. La fraude est polymorphe, et elle est partout. Si l'on cherche à évaluer individuellement chaque risque, cela devient très compliqué ; si l'on veut le faire de manière indépendante, sur chaque risque, par l'audit interne, ou un mixte audit interne/experts, cela devient très cher, très lourd, et la démarche risque de ne jamais s'engager.
On recommande donc l'approche suivante. **Une première étape** basée sur l'autoévaluation : identification des sites sur lesquels on veut poser une question spécifique, des interlocuteurs à qui poser ces questions. On demande à ces derniers de s'autoévaluer sur ces questions très spécifiques. Cela ne prend pas beaucoup de temps et, au fur et à mesure, cela va rentrer dans une démarche de fiabilisation et devenir de plus en plus pertinent et objectif. Le résultat de l'autoévaluation est blanc ou noir, 1 ou 0. Soit le risque est perçu comme fort dans l'autoévaluation, et on s'arrête là ; s'ensuit une décision du management qui accepte ou n'accepte pas ce risque, et s'il ne l'accepte pas, on détermine un plan d'action. De manière un peu spontanée, en autoévaluation, le plan d'action surgit. Soit le risque est perçu comme faible, et l'on peut alors se poser la question de la fiabilité de cette autoévaluation et déclencher une démarche dans une **deuxième étape**. Celle-ci consiste à procéder à une évaluation indépendante et donc sélective qui va s'intéresser à un échantillon des risques perçus comme faibles, pour apporter deux conclusions. La première, sur le niveau perçu de manière indépendante de l'exposition au risque de fraude ciblé : « On me disait que j'étais couvert. En fait, après analyse, je ne suis pas couvert. » La deuxième conclusion me donnera un avis sur la fiabilité de mon autoévaluation. La personne est très optimiste, me dit que tout va bien, mais quand j'ai revu avec elle son environnement, ses travaux, on est loin du compte. On lui apprend donc à faire son autoévaluation de manière plus fiable, l'année suivante, et les choses devraient s'améliorer.

Le premier élément que l'on essaie de faire évaluer à la personne concernée **est le risque inhérent**. On va lui poser quatre catégories de questions.
La première, sur son environnement de contrôle, sur l'évaluation du niveau éthique perçu dans son environnement : travaille-t-elle avec des gens plutôt intègres ou non ?
La deuxième, sur son niveau de pression, ses motivations ou des motivations perçues dans l'environnement, susceptibles de favoriser une fraude sur le site : y a-t-il une pression budgétaire forte, par exemple ? Y a-t-il une pression de par un environnement peu honnête ?
La troisième, sur les indicateurs de vulnérabilité. On va ici lui demander de se comparer par rapport à son secteur, à sa localisation, à sa taille : « Tous mes concurrents subissent ce type de fraude. Moi, je ne l'ai pas encore subi, mais a priori, je suis aussi exposé que les autres. » ou bien « Non. »
La quatrième, sur les incidents. Quel est le nombre des incidents remontés ? Quelle est leur nature ? L'incident est un révélateur de l'état des lieux et de la manière dont les gens fraudent.

Le deuxième élément, après le risque inhérent, **est l'appréciation du niveau de maîtrise qui permet d'aboutir au risque résiduel**. On demande, toujours à la personne concernée, de se positionner sur son contrôle interne, sur sa connaissance, sa perception des contrôles automatisés ou des contrôles portés par les systèmes d'information, et sur la séparation des tâches. Ces trois composantes clés lui

permettent de se dire : « Certes, je suis dans un environnement risqué, mais mon contrôle interne, mes systèmes d'information, ma séparation des tâches me permettent aujourd'hui d'être serein et je conclus sur mon niveau de risque perçu, résiduel, qu'il est faible, moyen ou fort. »

Si la personne répond : « J'ai un risque résiduel faible », on pourra, par l'analyse du risque inhérent, déclencher ou non un audit indépendant.
Cet audit indépendant est réalisé par une personne indépendante qui travaille avec ses schémas de fraude non communiqués à l'opérationnel, qui va les tester, et en tirer une conclusion.
Cette conclusion sera double : elle donnera à la fois un avis sur le niveau d'exposition et un avis sur la fiabilité de l'autoévaluation. Cela permet d'avoir une démarche sélective, donc moins onéreuse et plus efficace.

Beatriz SANZ REDRADO

La démarche que le groupe Galeries Lafayette a mise en place pour évaluer les risques, est assez classique : c'est une évaluation sur la probabilité et l'impact. Mais de plus, chaque grand risque de fraude identifié a été décortiqué en quatre paramètres.

Les schémas de fraude et d'indicateurs de fraude par processus.

Les moyens humains mis en oeuvre, pour surveiller ou identifier ces indicateurs. A ce stade, on a tendance à penser que c'est toujours la même configuration, et en fait, ce n'est pas vrai. Ainsi, il y a des branches où coexistent l'audit interne et le contrôle interne. Il y en a d'autres où il n'y a aujourd'hui ni audit interne ni contrôle interne. Il y en a certaines, beaucoup plus structurées, avec des contrôles permanents et des contrôles périodiques. Certains magasins ont des structures assez importantes, avec des directions de la sécurité, des contrôles ; des personnes affectées aux pertes et à tout ce qui peut avoir un impact sur la qualité des inventaires ; des personnes affectées à la sécurité, à l'entrée des magasins. Les moyens humains que l'on déploie doivent être proportionnels aux risques auxquels on est exposé. C'est là que l'on va identifier des écarts auxquels il faut remédier.

On a formalisé **les méthodes** de contrôle interne mises en place pour maîtriser les risques. On trouve ces méthodes dans deux pavés du COSO : l'environnement de contrôle interne et les procédures de contrôle interne. Cela concerne les structures, les contrôles (a priori et a posteriori), les applicatifs dans les systèmes d'information, les rapprochements, les validations, les délégations de pouvoir, les signatures… bref, toute une panoplie ; existe-t-elle ou non ?

Les outils de pilotage sont ceux dont le management dispose pour identifier les problèmes éventuels. On dispose très souvent de moyens et de méthodes, mais on n'est pas toujours à même de déceler un défaut de fonctionnement, sauf en cas de plainte. Il faut donc savoir quels sont les indicateurs et dans quelle mesure ces indicateurs sont pertinents, s'ils sont aisément utilisables, et de façon exhaustive et cohérente. Les mêmes indicateurs, dans deux unités différentes, peuvent vouloir dire des choses complètement différentes, parce qu'ils ont construits de façon différente. Une fois l'ensemble bien cadré, on peut passer à la cotation, cotation de la probabilité, cotation de l'impact.

On peut dire beaucoup de choses sur la probabilité : est-elle statistique ou non ? Est-elle mesurable ou non ? Je crois qu'il ne faut pas faire de montages trop compliqués. Pour moi, la probabilité est faible ou forte ; et si elle n'est ni forte ni faible, elle est moyenne.
La probabilité de survenance d'un risque de fraude est faible si celle-ci suppose un montage très complexe ou s'il faut la collusion d'un grand nombre de personnes. La probabilité est forte, lorsque le cas s'est déjà produit ou lorsque la fraude est extrêmement simple.

L'impact : l'impact financier et l'impact sur l'image de marque. On cote chaque risque en fonction de ces deux critères, et on retient la cotation la plus forte.

La question que l'on se pose toujours est : comment un auditeur peut-il appréhender les schémas de fraude ou les indicateurs de fraude ? La façon dont nous les appréhendons, au groupe Galeries

Lafayette, est assez simple. Soit l'information remonte (parce qu'il y a eu déjà des fraudes), par l'audit de branche, ou le contrôle interne, ou le contrôle permanent; soit parce que l'on fait de la veille avec des collègues ou du benchmark.
En réalisant des audits, on peut aussi identifier des risques de fraude. Ainsi, nous avons réalisé un audit de la chaîne logistique dans trois entrepôts, pour s'assurer que les flux de marchandises étaient sous contrôle. Deux entrepôts étaient très bien gérés, la gestion du troisième était catastrophique. Et pourtant, le directeur de l'entrepôt était persuadé que la fraude n'existait pas chez lui. Nous avons conduit notre audit normalement, avec le programme de travail qui avait déjà été validé à l'origine. Et l'on a constaté beaucoup d'indicateurs de fraude : il n'y avait pas d'indicateurs de pilotage, pas de reportings, et énormément de lacunes. Nous nous sommes demandé comment sensibiliser le management ; nous avons établi un diagramme (Ishikawa) sur lequel sont recensées toutes les actions qui peuvent conduire à un détournement d'actifs. Nous avons indiqué les actions urgentes à entreprendre pour sécuriser l'activité, et les actions moins urgentes mais nécessaires. La direction de la *supply chain*, la direction générale, et le comité d'audit ont beaucoup apprécié notre action, et ils ont fait prendre des mesures pour sécuriser les entrepôts. Voila un exemple très pratique de la manière dont l'audit interne peut apporter son savoir-faire à la gestion et au traitement du risque de fraude.

Autre exemple, beaucoup plus classique, sur les indicateurs de fraude, dans le processus achats. Les indices sont nombreux : absence de rotation de portefeuille des acheteurs ; absence de mise en concurrence ; absence de code éthique ; absence de séparation de tâches ; commandes enregistrées après réception de la facture… Naturellement on ajoute régulièrement les nouveaux risques identifiés.

Le troisième exemple concerne les diagrammes de flux que nous réalisons à l'occasion de nos missions d'audit interne, pour tout ce qui touche à la corruption et à la collusion, et notamment dans le cadre des appels d'offres.

Ces trois exemples donnent un aperçu de la façon dont l'audit peut cartographier et analyser la probabilité des risques de fraude et leur impact.

Sébastien ALLAIRE

Je voudrais insister sur la nécessité de documenter la démarche de cartographie des risques de fraude. Cette documentation peut se faire au moyen de fiches pour chaque risque majeur identifié. Elles peuvent être détenues par l'audit interne. Elles contiennent des informations plutôt confidentielles, qui ne sont pas forcément communiquées à l'ensemble de l'organisation. On y retrouve notamment des schémas de fraudes constatées.
Ces fiches doivent vivre. Nous pensons qu'elles doivent contenir trois types d'informations.
L'identification du risque : une sorte de fiche d'identité, l'ADN du risque. La définition claire du risque identifié ; les processus et les classes des comptes impactés ; les risques individuels et les facteurs de risques identifiés ; les schémas de fraudes identifiées.
L'évaluation du risque : la synthèse de ce qui aura pu remonter dans l'autoévaluation sur le risque inhérent, sur l'environnement de contrôle, et les acteurs ; les facteurs qui peuvent agir sur la réalisation du risque.
La maîtrise du risque : où en suis-je aujourd'hui sur ce risque ? Quel est le niveau de maîtrise apporté par le contrôle interne, les systèmes d'information, la séparation des tâches ? Quel est l'impact de vulnérabilité, le niveau de risque résiduel ? Quels sont les plans d'action ? Quel est le suivi de ces plans ?
Ces fiches sont la base de données fraudes. Elles servent de reporting au management.
Du fait de cette descente *top down* de manière ciblée, l'agrégation se fait de manière beaucoup plus systématique, beaucoup plus mécanique. On sait, en analysant les racines, à quel arbre elles appartiennent, on est donc rapidement en mesure de déterminer le risque de détournement

matériel sur stocks, sur immobilisations corporelles, sur cash, etc., et de présenter une vision synthétique du risque de fraude au management, et du positionnement précis des plans d'action.

Mais la cartographie des risques de fraude n'est qu'une première étape. On commence par se poser les questions sur l'exposition au risque, sur le caractère significatif du risque, et ensuite on se préoccupe de l'environnement et des renforcements éventuels. Puis, viennent les activités de contrôle, la sensibilisation et le pilotage du dispositif.

Il faut suivre l'évolution des risques : les risques naissent et meurent. La fraude est connue pour son aspect créatif. Il faut suivre les plans d'action : il ne sert à rien d'alerter le management sur un risque si ce n'est pas pour venir le rassurer dans quelques mois.

Le reporting sur les incidents doit être dynamique. Sachant qu'on apprend beaucoup des incidents, il faut positionner des capteurs dans l'organisation et analyser. La cartographie des risques, le management des risques de fraude, ne sont pas des systèmes sûrs à 100 %, et les fraudes continueront d'exister.
L'évaluation impact/fréquence doit être ajustée en permanence : certains risques, apparemment maîtrisés aujourd'hui, peuvent demain faire l'objet d'une reclassification dans la hiérarchie des risques.

Une présentation doit être faite, au moins une fois l'an, au comité d'audit de la cartographie des risques de fraude, du dispositif de gestion des risques de fraude et des plans d'action les plus significatifs.
On est là sur une logique de management. Le comité d'audit, comme le management, se préoccupe de l'exposition de l'entreprise au risque de fraude. Il est alerté, sur la fraude comptable et financière, par les commissaires aux comptes dans le cadre de leurs travaux. Le comité d'audit est également alerté par l'audit interne, qui a un spectre beaucoup plus large de fraudes potentielles comptables, financières et opérationnelles.
Le comité d'audit peut avoir des inquiétudes. L'intérêt de la cartographie des risques de fraude est de le rassurer en lui prouvant que le dispositif en place pour maîtriser les risques, pour prévenir la survenance de ces risques, est de plus en plus fiable. Ces éléments sont très importants dans une démarche de bonne gouvernance de l'entreprise.

Beatriz SANZ REDRADO

Quelques mots sur un retour d'expérience pratique.

Il est certain que **la fraude et le contrôle interne sont intimement liés**. Plus le contrôle interne est fort, plus il sera difficile de commettre une fraude ou de ne pas la déceler.
Le risque de fraude menace l'ensemble de l'entreprise, toutes les entités, tous les processus.
L'audit interne doit être proactif, identifier les problèmes et veiller aux renforcements nécessaires dans les contrôles.

Le fait d'établir **une cartographie du risque de fraude** a, pour moi, deux avantages. Le premier est d'appréhender le risque de fraude d'une façon globale, et le deuxième est de nous aider, nous, auditeurs, dans la réalisation de nos plans d'audit annuels, puisque notre analyse se fondera sur les principaux risques auxquels l'organisation est confrontée ou peut l'être.

Je citerai **trois bonnes pratiques** acquises en quinze années d'expérience.
Premièrement, on peut mettre en place les systèmes les plus performants, si l'on ne met pas les bonnes personnes aux bons postes, on a tous les risques de ne pas aboutir, et surtout concernant la fraude, sujet particulièrement délicat.
Deuxièmement, la disponibilité d'indicateurs et d'outils de reporting exhaustifs et fiables : je ne cesse de le dire, si l'on n'a pas d'indicateurs, on ne peut pas déceler les faiblesses et encore moins les fraudes. Il est donc très important de disposer d'indicateurs, de tableaux de bord, de benchmarks.

Troisièmement, il ne faut pas oublier que la direction générale et le conseil ont les moyens de donner une impulsion au traitement de la fraude et de ne pas la traiter comme un sujet tabou. Mais il faut savoir leur communiquer les informations dont ils ont besoin et sous une forme adéquate.
Dans une entreprise où je travaillais, il m'a fallu un an et demi pour comprendre les besoins de la direction générale, peu ou mal exprimés. Le jour où j'ai compris, je lui ai communiqué les informations sous une présentation différente. La direction a alors réagi et a fait prendre des dispositions pour lutter contre une typologie de fraude.

Jean-François SAUTIN

Dans un département d'audit, quel pourcentage des moyens affectez-vous à la cartographie des risques liés à la fraude, par rapport aux moyens globaux dont vous disposez ?

Beatriz SANZ REDRADO

A l'audit central que je dirige, les moyens humains sont peu nombreux puisque nous sommes neuf. On estime que nous passons environ 20 à 25 % de notre temps à lutter contre la fraude ou à mieux la comprendre.

A l'exception de quelques missions spécifiques, nos missions ne sont pas réellement liées à la fraude. Lorsque l'on identifie un risque de fraude très important – on a eu récemment le cas avec un site Internet que l'on a ouvert et que l'on s'est fait pirater –, on lance une mission globale. On ne traitera pas exclusivement du risque de fraude.
Nous estimons que le quart de notre temps est consacré à la réflexion. Lorsque nous identifions un risque de fraude, nous recherchons le contrôle interne qui fait défaut. Là est notre vrai travail.

Jean-François SAUTIN

Gérard Villard va maintenant nous parler de l'analyse des données : retour d'expérience de l'utilisation du logiciel ACL pour détecter les risques de fraude.
Gérard Villard est chez AXA France, et, depuis 2007, il est responsable de la gestion de crise et de la prévention des risques des activités opérationnelles.

L'ANALYSE DES DONNEES : RETOUR D'EXPERIENCE DE L'UTILISATION DU LOGICIEL ACL POUR DETECTER LES RISQUES DE FRAUDES PAR GERARD VILLARD

DPC – Prévention des risques des activités opérationnelles & gestion de crise, Direction de la sureté, AXA

La direction de la sûreté, dont je fais partie, dépend du secrétariat général d'AXA France.

La Sûreté dirige le traitement des incidents susceptibles de porter atteinte à la notoriété ou l'image de l'entreprise et qui sont de nature à constituer un risque humain, judiciaire ou financier pour l'entreprise, ses collaborateurs ou ses dirigeants. Elle sert : d'interface avec les autorités publiques et d'expert en Sûreté pour toutes les entités d'AXA France.

Elle comprend trois départements : les incidents distributeurs, le traitement des affaires sensibles et la gestion de crise, la prévention et le contrôle des risques opérationnels (LAB /LFT et lutte contre la fraude interne).

Les incidents distributeurs, c'est là que la fréquence de fraude était la plus importante, mais J'ai toujours été persuadé que c'est parce que l'on manquait d'outils sur d'autres compartiments de l'entreprise et, avec ACL, on a pu le démontrer.

Les incidents transversaux ou critiques, ces incidents ne concernent pas uniquement la fraude ; il peut s'agir d'incidents médiatiques, de harcèlement, de menaces physiques sur certains de nos salariés et de nos agents : lorsque l'on refuse à certaines populations le règlement d'un sinistre, les risques physiques sont réels.

La prévention et le contrôle des risques opérationnels, travaille sur la lutte contre le blanchiment et le financement du terrorisme, la gestion de crise, et la maîtrise des risques liés aux activités opérationnelles, concernant AXA France et les entités rattachées.

La direction de la sûreté a des correspondants dans toutes les directions ou entités rattachées (direction financière, DRH…) qui traitent des incidents de sûreté avec notre assistance.

Ne revenons pas sur la définition générale de la fraude. Aujourd'hui, nous nous intéressons à la fraude interne, c'est-à-dire celle qui est commise par un salarié de l'entreprise, un agent, un courtier ou un prestataire qui travaille pour le compte de l'entreprise … Aujourd'hui, nous n'encaissons plus nos chèques, , nous ne développons plus la totalité de nos logiciels : nous faisons appels en partie à des prestataires externes .

La fraude existe, l'entreprise, ses salariés et ses clients en sont les victimes. Elle n'est pas acceptable dans une société qui repose sur la confiance. Quand des détournements de fonds ont lieu, surtout dans une compagnie d'assurances ou une banque, la confiance et l'image sont réellement mises à mal.

Parallèlement à la position morale et éthique, la réglementation oblige les entreprises à se doter de dispositifs efficaces de lutte contre la fraude interne : c'est la loi LSF ; la NEP 240 qui demande, dans le cadre des audits de comptes, de rapporter les cas de fraude ; C'est la loi Sarbanes-Oxley : étant cotés à New York ; nous devons nous soumettre à des obligations locales ; c'est Solvabilité (*Solvency*) II pour les assurances et Bâle II pour les banques.
Ces obligations réglementaires s'imposent à notre société et nous demandent d'évaluer le niveau des risques opérationnels dont fait partie la fraude interne.

Le groupe et AXA France se sont donc équipés des moyens nécessaires pour répondre aux obligations : réglementation interne, codes de déontologie, outils de remontée d'incidents.

Ainsi, la direction de la sûreté va-t-elle traiter les incidents qui ont été déclarés et proposer des solutions pour réduire les risques. NORKOM, que nous mettons en place, est utilisé pour traiter le

blanchiment, et sera certainement utilisé aussi pour la lutte contre la fraude. Cet outil permet de traiter l'aspect comportemental, et les mouvements financiers sur un compte, exemple : si le compte d'un étudiant enregistre un grand nombre de mouvements de fonds en provenance ou en direction de l'étranger, il y a sans doute une anomalie.

La sûreté est également en charge de la prévention des risques opérationnels, dont la sécurisation des processus. Un département travaille sur tous les processus. Par exemple pour le recrutement, Nous avons produit un module de formation à destination des recruteurs pour améliorer le contrôle des références.

La sûreté déploie des outils comme ACL, au sein des services de contrôle interne. Nous avons différents services de contrôle interne, de contrôle permanent dans les différentes entités que j'ai citées tout à l'heure.

Une catégorisation des risques opérationnels a été définie au niveau du groupe. La fraude interne est un des risques opérationnels comme la fraude externe. Ce sont deux catégories de risques parmi sept catégories. Il y a ensuite vingt-deux sous–catégories, chacune d'entre elles étant subdivisée en cent événements. Notre reporting est construit sur ce niveau de détail.

Examinons la fraude interne. **Nous avons déterminé trois types de fraude interne** : le rapport financier frauduleux ; l'activité financière frauduleuse ou inappropriée ; le détournement d'actifs.

Rapport financier frauduleux : c'est l'omission et la dissimulation de données financières. C'est la falsification des comptes. Enron en est un bon exemple. La divulgation délibérée d'informations inexactes.

Les fraudes internes liées aux activités financières, c'est-à-dire des manipulations d'argent. C'est la divulgation délibérée d'informations sensibles, les délits d'initiés, le transfert de compte à compte pour masquer des informations.
Nous avons eu des cas de détournements de fonds par des salariés, des prestataires ; des détournements de chèques volés et remis à l'encaissement au Luxembourg etc.

Les détournements d'actifs. Le détournement d'actifs est le vol de matériel, la complicité pour des sinistres fictifs, la contrefaçon ou la falsification etc.

Comment procède-t-on pour détecter la fraude ? Il faut d'abord déterminer quelles sont les zones sensibles, c'est-à-dire non ou difficilement contrôlées. Ce sont d'une part les procédures manuelles non standardisées. Notre société a connu beaucoup de fusions, et par conséquent des fusions d'activités issues de sociétés diverses. Avant que les standards soient mis en place, avant que les systèmes d'information soient adaptés à la nouvelle organisation, un certain nombre d'activités restent manuelles qu'il est évidemment plus difficile à contrôler. Ce sont, d'autre part, les modifications législatives et réglementaires dont l'intégration dans nos systèmes demande des délais ; nous sommes donc obligés de faire des « bistouris informatiques » pour pouvoir les intégrer rapidement ; ces développements temporaires facilitent la mise en œuvre de fraudes. Ce sont aussi les entités à faible turn over, La mobilité, assez répandu au sein d'AXA, peut favoriser les risques de fraude lorsqu'un manager découvre une activité, alors que l'équipe en place a de l'ancienneté et connait les faiblesses de l'organisation dans laquelle elle travaille.

Autres zones sensibles : les activités d'encaissement et de décaissement ; les activités comptables (falsification des comptes) ; les activités commerciales ; les services informatiques dans lesquels le détournement de règles est assez facile ; les fonctions achats.

Etat des lieux et statistiques. Des statistiques externes font état pour l'ensemble des activités économiques d'un taux de fraude d'origine interne de 80%. Je relativise un peu en ce qui concerne l'assurance : 80 % de la fraude est externe : il est notoire qu'une grande proportion des assurés a tendance à gonfler les sinistres. Pour notre secteur d'activité, la fraude externe est donc beaucoup plus importante que la fraude interne.

Chez AXA France, nous disposons d'un outil, RTI, qui permet de faire remonter l'ensemble des incidents survenus dans les différentes entités, via nos correspondants. C'est à la fois un outil déclaratif, et un *workflow* de gestion des incidents. Cela ne veut pas dire que l'on mesure toute la fraude interne grâce à cet outil, que tous les incidents sont dans RTI, mais c'est en tout cas un bon indicateur.
60 % des incidents enregistrés dans cet outil sont des cas de fraude interne.
Six millions d'euros de fraude ont été traités en 2008, par la direction de la sûreté. Ce chiffre peut paraître important mais il représente moins de 4 ‰ de notre résultat opérationnel qui était de 1,268 milliard. D'autre part, une partie de l'argent détournée est récupérée même si dans certains cas le processus est lent.
Mais il n'y a pas que l'impact financier : les impacts d'image, les impacts sociaux, judiciaires, peuvent être lourds.

L'environnement de contrôle.
C'est d'abord une affirmation des valeurs de l'entreprise (honnêteté, intégrité…).
Les « *group anti-fraud standards »* s'appliquent à l'ensemble des filiales AXA dans le monde ; ils définissent les standards en termes de communication, mais aussi d'outils et de reporting.
Dans le code de déontologie AXA France, une partie est dédiée à la fraude interne. Des guides d'éthique sont déclinés par métier.
Un déontologue, au sein d'AXA, a pour rôle de définir avec l'ensemble des interlocuteurs sur la façon de traiter tous les problèmes liés à la déontologie.
Il y a le comité d'audit.

La prévention.
Ce sont les notes de procédures, les instructions, le contrôle interne.
L'analyse du risque de fraude interne dans les projets et les modifications de procédures. AXA France Service, qui est, je vous le rappelle, l'entité d'organisation et d'informatique, a prévu pour les nouveaux projets, des supports d'analyse concernant le domaine de la fraude informatique et de la fraude en général.
Pour le recrutement, il existe un recueil et un contrôle des références.
La hiérarchie est impliquée dans la vigilance. Nous réalisons des campagnes de sensibilisation. Tous les commerciaux salariés qui arrivent au centre de formation, rencontrent la direction de la sûreté pendant une demi-journée. Nous parlons de la lutte contre le blanchiment des capitaux, mais aussi de tous les dispositifs que nous mettons en place pour lutter contre la fraude. Ils savent donc qu'il existe une direction dédiée à la détection et au traitement des fraudes internes. C'est une mesure de dissuasion.
La sécurisation de l'accès aux moyens de paiement : nous avons supprimé pratiquement toutes nos caisses, et nous mettons en place des dispositifs qui permettent de diminuer le risque pour les autres flux financiers.
La séparation de fonctions est une des premières mesures que l'on doit mettre en place, elle est cependant assez difficile à respecter pour des unités de très faible taille.

La **détection** est assurée par différents corps de contrôle.
Les missions d'audit : les commissaires aux comptes, l'audit interne, l'ACAM (l'organisme de tutelle qui contrôle les compagnies d'assurance et les mutuelles), la direction de la sûreté.
La mise en place d'outils de contrôles exhaustifs : ACL a permis de détecter des fraudes parmi les salariés des agents généraux et chez nos courtiers. Norkom est utilisé dans la lutte anti blanchiment, mais on pense aussi l'utiliser pour la fraude interne. D'autres outils sont mis en place pour la gestion des imprimés, et notamment les cartes vertes, car ce sont des documents facilement monnayables.
Des contrôles actifs par des services dédiés au contrôle a posteriori : le service réclamations clients est un des acteurs importants de détection de la fraude : une partie des incidents qui remontent à la direction de la sûreté, ont pour origine une réclamation anodine d'un client. D'autres services font des analyses techniques des comptes de nos agents.

Le **signalement**, c'est-à-dire le fait de faire remonter des opérations bizarres ou peu claires par l'outil RTI. Il existe aussi une ligne éthique, qui n'est pas anonyme, et qui permet aux salariés, en France, de déclarer au groupe – et pas à AXA France – les incidents de type financier.
Un médiateur indépendant arbitre entre nos services de gestion et le client. Dans certains cas, on se rend compte qu'il y a eu fraude. Le service réclamations.

Je vais maintenant parler de **l'outil ACL** et dire en quoi l'outil a apporté énormément dans la lutte contre la fraude.

C'est d'abord un outil qui permet de traiter des volumes illimités de données. Pour vous donner un exemple, le premier traitement que nous avons réalisé portait sur une chaîne de décaissement, sur trois ans, et représentait treize millions de lignes.
Autre avantage : les traitements sont assez rapides. Quand je dis « assez rapides », cela veut dire de quelques minutes à quelques heures. On traite les données en direct sur son portable et on a l'avantage d'avoir tout de suite des résultats et de pouvoir ajuster les traitements.
ACL accède aux données en lecture seule, cela a un gros avantage pour sécuriser et surtout rassurer les informaticiens sur la gestion de leurs propres données. Les données et les traitements ne sont intimement liés comme sur un tableur.
Fonctionnalités spécifiques d'audit : il y a quelques outils, à l'intérieur d'ACL développées spécifiquement pour l'audit.
L'indépendance par rapport aux ressources informatiques : accès immédiat aux données sources sans recourir à des extractions et à la redéfinition de données longues et complexes.
Lorsque l'on analyse un problème précis, ACL enregistre tout ce que l'on fait. Cela a un intérêt du point de vue de la traçabilité lors d'une mission d'audit, mais aussi quant à la constitution de scripts que l'on pourra réutiliser pour de prochaines études sur une activité assez semblable. On pourra construire, à travers des scripts ACL, des moyens d'améliorer le contrôle permanent sur l'ensemble des transactions traitées par les unités opérationnelles.
La vérification exhaustive : l'ACL enregistre la totalité des commandes et des résultats, et crée ainsi une piste de vérification exhaustive. En matière de preuve sur les résultats obtenus, c'est assez précieux pour l'audit.

Sur quoi avons-nous travaillé à la direction de la sûreté ?
D'abord sur les dates d'événements. Dans une compagnie d'assurance ou dans une banque, pratiquement toutes les transactions sont horodatées. Il est intéressant d'étudier les allers et retours sur certaines opérations : changements de nom, d'adresse, d'immatriculation, ayant pour but de détourner des courriers. On constate aussi des sinistres intervenant très peu de temps après la souscription, des opérations rétroactives, des collusions probables entre le distributeur et l'assuré, des modifications de RIB pour détourner des règlements, etc.
Ensuite sur des données partagées entre plusieurs personnes : est-il normal que des assurés ne reçoivent pas des règlements qui leur sont destinés, et que ces règlements aillent vers d'autres personnes ? Est-il normal que plusieurs personnes, plusieurs contrats aient des adresses identiques, des dates de naissance identiques, des immatriculations identiques ? etc.
Le fait de pouvoir travailler sur la totalité des données et non plus sur des échantillons nous donne la garantie de déceler à coup sûr toute anomalie existante. Ce type d'outil, très réactif, est motivant, en ce qu'il donne le moyen de ne rien laisser passer.

Sur quoi travaillons-nous maintenant ?
Nous sommes actuellement en train de travailler sur la réutilisation des études que nous avons effectuées pour créer des scripts que nous allons livrer dans les directions opérationnelles, de façon à ce que les traitements *one shot* réalisés par notre direction soient réutilisés de façon récurrente au sein des directions opérationnelles. C'est un gros travail d'analyse informatique à mener pour offrir des scripts de type « presse-bouton ».

Notre plan d'action pour lutter contre la fraude interne comporte trois axes.
Premier axe : réduire l'incitation en renforçant la surveillance.

Il faut donner des outils à l'encadrement ; sensibiliser à la fraude interne ; former sur la manière de détecter une fraude ; l'outil RTI, désormais disponible dans l'ensemble de nos filiales, permet de gérer les incidents ; éviter d'intégrer, dans les activités sensibles, des personnes non permanentes de l'entreprise ; développer le contrôle continu (SOX, ACL…)
Il faut améliorer la gestion RH des individus ; maîtriser le recrutement et faire évoluer régulièrement les personnes sur les postes sensibles.
Il faut rappeler aux collaborateurs les bonnes pratiques en matière de contrôle interne : ne pas divulguer son mot de passe ; effectuer les contrôles définis dans les processus ; signaler les anomalies qui ne trouvent pas d'explications ; rappeler fréquemment qu'il existe des outils permettant de faire remonter les anomalies.

Deuxième axe : réduire l'opportunité en améliorant le contrôle interne.
D'abord organiser le dispositif de détection : mettre en place une cartographie des risques et des contrôles, et identifier les responsables de chaque contrôle.
Ensuite piloter les dispositifs de détection : prioriser les actions en fonction du risque ; assurer la traçabilité et le reporting du contrôle ; mettre en place des plans d'amélioration ; systématiser la séparation des tâches ; effectuer la remontée des incidents (ligne éthique, RTI, managers).

Troisième axe : réduire la capacité à rationaliser.
Il faut encore rappeler les valeurs éthiques. Rappeler quels sont les impacts, qui ne sont pas seulement financiers. Il faut aussi rappeler, lors des fréquentes sensibilisations que nous faisons auprès du personnel, quelles sont les sanctions pénales encourues ; on ne citera pas de noms, mais on peut faire état de condamnations récentes. On rappellera enfin les sanctions internes : retrait de mandat, licenciement…

Chez AXA France, désormais nous complétons la détection basée sur des échantillons par des contrôles exhaustifs, avec NorKom, pour la lutte anti blanchiment et avec ACL pour les risques opérationnels.

QUESTIONS/REPONSES

Jean-François SAUTIN

J'ai une question : vous n'avez pas prononcé le mot magique de CNIL. Comment cela se passe-t-il quand vous utilisez ACL, quand vous faites des recherches par nom, par personne ? Etes-vous soumis à une autorisation préalable de la CNIL ?

Gérard VILLARD

Non, parce que tous les traitements que nous faisons ont déjà été déclarés dans le cadre de nos systèmes d'information. Ainsi nous n'avons pas déclaré le fait de trier l'ensemble des règlements par compte bancaire. Mais, dans nos systèmes d'information, nous avons déjà la possibilité de faire ce type de traitement (mais de façon moins souple).Notre CIL (correspondant informatique et libertés) est assez tatillon.

Question

Je voudrais poursuivre sur la CNIL. Quand vous avez évoqué tout à l'heure le recrutement, vous disiez qu'il ne fallait pas recruter des fraudeurs, enfin des gens qui avaient pu frauder.

NB : ACL n'est pas utilisé pour le recrutement et le contrôle des références ne fait pas appel à un traitement informatique

Gérard VILLARD

On essaie, en tout cas, oui.

Question

Je m'interrogeais sur la constitution de sortes de *blacklists*.

Gérard VILLARD

Nous n'avons pas de *blacklist*. Dans le contrôle des références, sont indiquées les bonnes pratiques à exercer pour contrôler les dires du candidat. On avertit ce dernier qu'il sera soumis au contrôle des références, et on lui demande d'ailleurs qui l'on peut contacter dans le cadre de ce contrôle des références.

Il existe un certain nombre de pratiques et de moyens aujourd'hui pour s'assurer que la personne qui déclare des diplômes, les a réellement ; qui déclare avoir quitté tel employeur, pour telles raisons, ne raconte pas d'histoires.

TABLE RONDE : LE PROCESSUS DE CERTIFICATION : QUELS EN SONT LES PRE-REQUIS ?

ANIME PAR **NOËL PONS,** *CONSULTANT ;*

AVEC **FREDERIC GEOFFROY**, *RESPONSABLE AUDIT INTERNE, SGCIB ;*

MARIANO MARCOS, *ASSOCIE, PRICEWATERHOUSECOOPERS ;*

HELENE PLOIX, *PRESIDENT DE PECHEL INDUSTRIES PARTENAIRES, PRESIDENT DE COMITES D'AUDIT ;*

JEAN-FRANÇOIS SAUTIN, *SENIOR VICE-PRESIDENT GROUP AUDIT, LAFARGE ;*

Noël PONS

Nous allons ouvrir la table ronde : quels processus de gouvernement d'entreprise mettre en place pour gérer le risque de fraude ? C'est un sujet important, puisque c'est de ce type d'organisation que va dépendre la réalité de la prévention et des travaux qui pourront être faits sur la fraude.

Nous traiterons divers sujets. Nous allons tout d'abord revenir sur la définition de la fraude : qu'entend-on réellement par fraude ? Nous verrons ensuite quels processus de gouvernement d'entreprise, quelle organisation mettre en place pour gérer ce risque, qui est un risque spécifique. Ensuite, quel est le rôle de l'audit interne, dans la détection de la fraude ? Enfin, quels dispositifs de suivi et de reporting permettent de lutter efficacement contre la fraude ?

Sont réunis, autour de cette table ronde, quatre intervenants.

Hélène Ploix. Elle est actuellement président de Pechel Industries Partenaires.
Mariano Marcos est associé de PricewaterhouseCoopers, responsable des activités de conseil dans le domaine de la trésorerie et des risques financiers.
Frédéric Geoffroy est un pur produit de la Société Générale. Il est actuellement directeur de l'audit corporate de la banque d'investissement.
Jean-François Sautin est un pur produit de Lafarge. Il est actuellement responsable des services du groupe Audit.

Mme Ploix, qu'entend-on par fraude ?

Hélène PLOIX, *Président de Pechel Industries Partenaires, Président de Comités d'audit*

C'est un acte illégal, commis intentionnellement, en vue d'obtenir un gain indu. Tous les éléments ont déjà été donnés en début de session et résument parfaitement ce qu'est une fraude.

Noël PONS

La fraude est un élément extrêmement complexe, dans la mesure où l'on fait intervenir à la fois des problématiques de faille dans les processus, des risques pénaux, des risques civils et des risques commerciaux.
Maintenant, je vous pose une deuxième question : quelle organisation mettre en place pour gérer le risque de fraude ? Votre expérience laisse entendre que vous avez parfaitement organisé les choses.

Hélène PLOIX

Je vais vous raconter une histoire vraie, l'organisation que j'ai contribué à mettre en place dans une entreprise que je dirai moyenne-grande, puisqu'elle compte environ 3 000 salariés, est répartie sur plus de 35 pays et fait entre 800 millions et 1 milliard d'euros de chiffre d'affaires.
Je décrirai **le processus en trois phases** qui me paraissent fondamentales. **La première est une phase organisationnelle**, qui commence par un point auquel je suis très attachée : le *tone at the top*. Il faut que l'exemple vienne d'en haut. Dans tous ces domaines liés à l'éthique, au bon comportement, il faut que l'exemple soit donné par les cadres dirigeants.
En l'occurrence, le président de la société a décidé un jour – sa société n'est pas très ancienne, mais elle a quand même une bonne vingtaine d'années – de définir une philosophie pour l'entreprise, un certain nombre de valeurs et une explicitation de ces valeurs dans les bons comportements. Tout ceci a été défini dans le cadre du groupe de direction générale, ce que je crois être une bonne chose. Certes, on peut demander à tous les salariés d'y contribuer, mais l'exemple vient d'en haut et il est fondamental qu'il y ait une profonde adhésion au sommet sur ce que l'on pense être les valeurs de l'entreprise et comment elles doivent se décliner dans le cadre des activités de l'entreprise.
Dans le même temps, il a été décidé de créer un comité issu du conseil d'administration pour suivre ces sujets. Et, comme la charte existait, comme les valeurs étaient connues, la conclusion a été : « Il faut que, si quelqu'un dans l'entreprise constate que ces valeurs ne sont pas bien appliquées, que quelque chose est distordu, il faut que cette personne ait la possibilité de le dire. », cela impliquait la mise en place du *whistleblowing* et la recherche du système le plus adapté de suivi et prise en compte du *whistleblowing*. Pour mettre en place un système de *whistleblowing* sur plus de 35 pays, il fallait que quelqu'un s'en occupe presque à plein temps. Le conseil a donc nommé un *Ethics Officer*, quelqu'un qui, dans l'organisation, était très respecté, avait un très grand sens des relations humaines, était très respectueux des valeurs et avait un comportement irréprochable.
Voilà l'organisation mise en place : *tone at the top*, comité du conseil et un *Ethics Officer*.

Phase suivante : faire adhérer l'ensemble de l'entreprise, lui faire comprendre ce que cela signifiait, les comportements à adopter, comment réagir dans la vie quotidienne de l'entreprise.
La première étape, dans cette deuxième phase, a été de faire adhérer l'ensemble de l'encadrement à ces valeurs, à cette philosophie. Pendant un an, dans toutes les réunions – les réunions des responsables financiers, des managers d'entité, des responsables des ressources humaines, etc. – du temps de parole a été donné à l'*Ethics Officer* pour qu'il explique la philosophie de l'entreprise, ses valeurs, et comment agir pour qu'elles soient appliquées et respectées dans l'entreprise.
La deuxième étape a consisté à s'assurer que tout le monde était bien informé.
La troisième étape a été la formation de tout le personnel : formation des nouveaux venus ; formation des managers pour qu'ils répondent de façon satisfaisante à leurs employés ; formation des responsables des ressources humaines. Comment cette formation a-t-elle était faite ? A partir d'études de cas. Des cas d'une page, deux pages, qui mettent en évidence un dilemme, une question, que ce soit dans la relation avec un client, dans la relation avec un fournisseur, dans les relations entre personnes de l'organisation, que ce soit dans l'utilisation de l'information de l'entreprise – et surtout dans sa non-utilisation vis-à-vis de l'extérieur.

La troisième phase c'est de faire vivre ce système. Pour cela, il y a un certain nombre d'outils. D'abord, le mécanisme de *whistleblowing* pour lequel il a fallu près de deux ans pour le mettre au point, car il devait être acceptable dans chaque pays. Vous savez qu'avec la CNIL, en France, on ne peut pas tout faire. C'est encore plus compliqué en Belgique. En Italie, ce n'est pas très facile. Et je ne vous parle pas des difficultés dans des pays plus éloignés, en Amérique latine ou en Europe de l'Est.
Il a donc fallu étudier la réglementation de chacun des pays et adapter le mécanisme pour qu'il soit acceptable légalement dans le pays. Il a fallu rédiger une documentation dans la langue du pays. Un ensemble de documents promotionnels (affiches, livrets) concernant la ligne de *whistleblowing* a été développé, expliquant le fonctionnement.

Tout à fait récemment, maintenant que le système est en place, la société a diffusé, dans l'ensemble de ces pays et à tous les employés, une lettre expliquant que l'utilisation de cette ligne ne peut les mettre pas en risque.
Dans le même temps, pour entretenir le système, ont été développés des « petits cas », que l'on appelle les *Ethics Dilemmas*. Ils ont été travaillés, réunis dans un opuscule, et postés sur l'intranet. Tout un volet de l'intranet parle de l'organisation, du mode de fonctionnement du *whistleblowing* ; il reproduit des documents comme la charte éthique de l'entreprise.
Dans chacun des pays, il a été proposé aux dirigeants de nommer un correspondant éthique. Cette proposition a été extrêmement bien accueillie. Une personne s'acquitte de cette charge en plus de son travail. Il n'y a aucune rémunération, aucun temps imparti. Elle est l'interlocuteur de l'*Ethics Officer* pour garantir le respect des valeurs de l'entreprise.

Maintenant, tout ce système fonctionne. Très régulièrement, des éléments remontent de la ligne de *whistleblowing*. Ce sont souvent, je ne vous le cache pas, des problèmes de relations humaines, de personnes, mais qu'il faut connaître au niveau central, parce qu'ils révèlent parfois de réels problèmes d'organisation et de management. Et, comme l'*Ethics Officer*, vers lequel ces sujets remontent, en a une très bonne compréhension, il sait très bien vers qui se retourner pour qu'ils soient traités. Ce sont soit des sujets de fraude, et on se tourne alors vers l'audit interne ; soit des sujets managériaux, et on se tourne vers la personne la plus adaptée pour les régler ; soit des questions de droit du travail, etc., et on se tourne vers les ressources humaines.
Les trois piliers du système sont : l'*Ethics Officer*, élément clé évidemment ; l'audit interne, qui joue un rôle de premier plan dans les investigations ; l'*Ethics Committee*, qui se réunit quatre fois par an et qui rapporte au conseil sur ces sujets.
Voilà une organisation qui veut, de haut en bas, créer un système de valeurs qui éloigne (théoriquement) toute idée de fraude, mais aussi, de bas en haut, donne la possibilité de détecter les fraudes éventuelles, soit au travers du *whistleblowing*, soit au travers du contrôle interne.

Noël PONS

Jean-François Sautin, compte tenu de la dispersion des sites et de la diversité des métiers, quelle politique de lutte contre la fraude avez-vous mis en place dans votre structure ?

Jean-François SAUTIN

Je vais vous parler d'un univers très industriel comparé aux univers dont on a parlé jusqu'alors. Lafarge est le leader mondial des matériaux de construction, avec trois métiers : ciment, béton et granulats, plaques de plâtre. Un chiffre d'affaires de 19 milliards d'euros ; une présence dans 79 pays ; 84 000 collaborateurs ; 166 cimenteries ; 1 300 centrales à béton.

Avant d'être responsable de l'audit interne, j'ai eu des responsabilités opérationnelles, jusque en 2006. Pour moi la fraude était un phénomène quasi naturel. Les cas étaient traités plutôt à l'initiative des opérations locales, jusqu'à ce qu'il y ait une prise de conscience, en centrale, évidemment liée à la certification Sarbanes-Oxley – disons en 2004 –, la mise en œuvre d'un univers d'analyse du contrôle interne beaucoup plus structuré qu'il ne l'était auparavant et homogène dans l'ensemble du groupe, et la création, entre autres, d'une *Whistleblowing Line*. Bref, un certain nombre d'actions très claires, et l'écriture d'un *Code of business conduct* qui renforçait les principes d'action du groupe. Lafarge a une gestion culturelle au travers de principes d'action depuis très longtemps, mais nos principes d'action n'étaient pas particulièrement focalisés sur la fraude. Je dirai très simplement, très naturellement qu'il est beaucoup plus intéressant de parler de stratégie, de développement de business, de technique, que de parler de choses un peu troubles comme la fraude. On n'en parlait pas tellement en interne.

Sarbanes-Oxley a été l'occasion d'une prise de conscience sur le contrôle interne et, par conséquent, sur la fraude.
Dans le même temps, nous avons adopté une politique de reporting de la fraude qui précisait le rôle des différents acteurs, rappelant, d'entrée de jeu, que ce sont les opérationnels qui sont en première ligne. En outre, a été décidée l'obligation de faire connaître en centrale tous les cas de fraude dans le groupe, sans seuil de matérialité, afin de faire un état des lieux, le plus complet possible, du groupe en matière de fraude, comprendre les problématiques, et pouvoir ajuster les contrôles en conséquence.
Dans le cadre Sarbanes-Oxley, nous avions entre autres – et j'y reviendrai un peu plus tard – l'obligation de produire une lettre de certification. Chaque patron de filiale faisait un état des lieux de sa filiale, une fois par an, à la fin de l'année, pour la certification des comptes, et faisait remonter à sa hiérarchie une déclaration des cas de fraude dont il avait eu connaissance, et des manquements au code de conduite des affaires. Cette méthode, très anglo-saxonne pour un groupe qui n'était pas très anglo-saxon, nous semblait somme toute assez intéressante.

Nous nous sommes délistés de New York et nous ne sommes donc plus soumis aux obligations de Sarbanes-Oxley. Toutefois, ces éléments-là ont été conservés comme un des fondamentaux du groupe en matière de contrôle interne.

Noël PONS

Frédéric Geoffroy, en tant que responsable de ce problème dans le cadre bancaire, pouvez-vous nous dire s'il existe une méthodologie et des structures spécifiques dans ce domaine ? Ou suit-on le schéma classique ?

Frédéric GEOFFROY, *Responsable Audit interne, SGCIB*

Je vais surtout m'exprimer comme représentant du groupe de travail qui a été constitué par l'IFACI pour rédiger un cahier de la recherche sur la fraude, groupe de travail qui a réuni les principales banques de la place.

Comme il a été dit, la fraude dans la banque est un sujet naturel. C'est aussi un sujet ancien, qui, en France, concernait jusqu'à présent surtout la banque de détail et le crédit à la consommation. Mais, de manière regrettable, depuis deux ans, c'est un sujet qui est devenu beaucoup plus actuel, et sur lequel les banques ont dû porter un regard neuf.
Suite aux événements, la commission bancaire a demandé expressément la mise en place de dispositifs spécifiques et la nomination d'un responsable de cette mise en place. Danièle Nouy est intervenue il y a exactement un an, dans le cadre d'une rencontre entre l'IFACI et les banques, et elle a été très claire sur le sujet.

Pour la confection du cahier de la recherche sur la fraude, nous avons décidé d'établir un benchmark des bonnes pratiques et des organisations mises en place par les différentes banques. La question était « Avez-vous créé ou avez-vous l'intention de mettre en place des équipes dédiées à la prévention et à la lutte contre la fraude ? »
Nous avons établi un questionnaire autour des sujets suivants : existence ou non d'une ou plusieurs équipes dédiées à la lutte et à la prévention contre la fraude ; organisation et direction de l'équipe ; ordre de mission de l'équipe ; prévention contre la fraude ; techniques de prévention contre la fraude ; techniques de remontée ; organisation des alertes ; techniques et programmes de détection et d'investigation ; éventuellement, logiciels utilisés.
Ce questionnaire a été adressé aux principaux établissements bancaires opérant en France et les participants au groupe de travail l'ont complété d'un certain nombre d'observations, en fonction des connaissances qu'ils pouvaient avoir des pratiques d'établissements étrangers, en particulier aux Etats-Unis et au Royaume-Uni.

Le constat est que tous les établissements ont mis ou vont mettre très prochainement en place des équipes dédiées à la prévention, à la détection de la fraude et parfois à l'investigation. Toutes les banques ont donc décidé de mettre en place des solutions spécifiques, ce qui implique des dispositifs, des responsables, des procédures...
Ces équipes sont pour l'instant de taille réduite, avec des profils expérimentés. Leurs lettres de mission sont très similaires : détection, prévention, sensibilisation des opérationnels – c'est un point très important –, tous les aspects formation, remontée des alertes, centralisation des alertes, analyse des cas de fraude, pour en tirer des enseignements et mettre en place des mesures de prévention.

Si les lettres de mission sont très généralement similaires, des solutions diverses ont été mises en place et on constate une grande hétérogénéité des modèles d'organisation. Le rattachement est soit hiérarchique, soit fonctionnel à la Conformité. On trouve également des rattachements au CEO, au responsable de la sécurité, ou à la direction des risques, et éventuellement, au sein de la direction des risques, à un département risques opérationnels.
L'organisation elle-même peut être centralisée ou complètement décentralisée, chaque branche, compte tenu de ses spécificités ayant décidé de mettre en place un service de prévention de la fraude.
La coordination est assurée soit par la compliance, soit par la direction des risques, et il y a des niveaux d'intervention et des dotations en effectifs variables selon la nature des risques audités.
Les pratiques en matière de détection sont assez similaires : utilisation d'outils de *data mining* ; exploitation des alertes remontées par les opérationnels, par le contrôle de premier niveau ou par le contrôle périodique ; contrôles inopinés pouvant être effectués soit par l'équipe antifraude, soit par le contrôle périodique qui doit travailler en étroite collaboration avec la cellule antifraude.
Les investigations sont généralement effectuées par le contrôle périodique, audit ou inspection générale. Dans un certain nombre de cas, cependant, c'est l'équipe que j'appellerai antifraude qui procède à ces investigations, surtout pour les cas de fraude les plus courants. On peut aussi trouver un mix des deux : on associe un élément de l'équipe antifraude et le contrôle périodique.
Les procédures de *whistleblowing* sont mises en place dans tous les établissements qui ont répondu au questionnaire.

Des dispositifs spécifiques, une montée en puissance de ces dispositifs, une coopération étroite avec le contrôle périodique, mais des solutions très diverses, très hétérogènes. Les modèles doivent gagner en maturité pour que l'on puisse véritablement dégager une bonne pratique.

Noël PONS

Mariano Marcos va nous expliquer quelles sont les autres conditions de l'efficacité d'un dispositif de lutte contre la fraude au regard du contrôle interne.

Mariano MARCOS, *Associé, PricewaterhouseCoopers*

Avant tout, pour disposer d'un dispositif qui fonctionne, il faut définir une politique de gestion de son risque de fraude, structurer son organisation, définir le rôle et les responsabilités de chacun, dissiper tout malentendu sur les prérogatives individuelles, surtout lorsqu'il s'agit d'une grosse entreprise ou d'une institution financière de taille respectable.
Une fois la politique déterminée, la clé est la communication. Communication autour de cette politique, faire savoir qu'elle existe, et surtout qu'elle va être suivie d'effets, qu'il y aura des reportings réguliers sur l'organisation et les actions menées ; prouver qu'un certain nombre d'actions, de recherches, d'investigations, d'analyses d'indicateurs ont été effectuées et ont porté leurs fruits, tant pour évaluer les probabilités de risque de fraude dans l'entreprise que pour identifier éventuellement des fraudes effectives.

Cela passe bien sûr par les moyens : moyens humains, outils. Dans nombre de fraudes, des indicateurs avaient fonctionné, des contrôles avaient été effectués, mais faute d'avoir été poussés, ils n'ont pas permis de déceler la fraude : voir le cas Madoff. Si l'on veut aller au fond des choses, il faut une équipe disponible, une équipe d'experts, une équipe capable de garantir une certaine indépendance vis-à-vis du business.

Un dispositif efficace, c'est un dispositif adapté. On peut mettre beaucoup de moyens sur l'analyse de certains indicateurs, mais si ces indicateurs se révèlent peu pertinents, les moyens sont mal utilisés. Dans certains cas, si un indicateur n'est pas croisé avec un ou plusieurs autres, sa pertinence est douteuse. Etre adapté, c'est aussi s'adapter à la géographie. Un dispositif qui fonctionne bien en France, fonctionnera peut-être moins bien dans des pays étrangers, où les us et coutumes, les pratiques commerciales, les circuits de paiement ne sont pas les mêmes, et requièrent donc une connaissance et une appréciation différentes des risques de fraude.
Un dispositif efficace est aussi un dispositif qui est maintenu, même quand les aléas externes sont défavorables. Par les temps qui courent, la recherche d'économies prime et on se contente parfois des dispositifs réglementaires, sans aller au-delà, se privant ainsi de certains moyens pour réaliser une gestion des risques de fraude efficace et efficiente.

Il faut faire preuve de souplesse et d'adaptabilité puisque, on le sait, les entreprises modifient leur structure en permanence, du fait des fusions, des restructurations, des absorptions. Le dispositif de gestion du risque de fraude est souvent le parent pauvre de la restructuration. Il est un peu oublié dans tout le dispositif. On pense plus à la consolidation, à la trésorerie, au commercial, au marketing.

Je reprendrai la formule d'Hélène Ploix, le *tone at the top*. C'est, je pense, la pierre angulaire. L'exemplarité des dirigeants est la condition clé de l'efficacité d'un dispositif. Si l'exemple ne vient pas d'en haut, tout l'édifice perd de sa valeur et de sa consistance, même en mettant un certain nombre de moyens.

Noël PONS

Et plus généralement, y aurait-il une sorte d'édifice idéal ?

Mariano MARCOS

D'organisation idéale ? Vous imaginez bien que non, étant donné la disparité de taille des entreprises, leurs problématiques sectorielles, leur déploiement géographique qui sont très différents et qui ne leur permet donc pas de mettre en place, chacune, un dispositif idéal. En revanche, il y a quelques points sur lesquels les PMI/PME peuvent s'appuyer.
C'est, en premier lieu, l'exemplarité des dirigeants et du management. Le premier rempart est la sensibilité des managers à leurs risques et donc leur habileté à capter le risque de fraude, parce qu'ils sont à la fois proches du business et proches des collaborateurs. A eux de délimiter les zones à risque et de s'y concentrer, même s'ils ne peuvent pas traiter toutes les zones à risque, du fait de la multiplicité de leurs fonctions.

Noël PONS

Ils sont obligés de prioriser.

Mariano MARCOS

Exactement.

Je pense aussi que le point clé, pour eux, est de s'appuyer sur les tiers. Un certain nombre d'informations leur viennent de leurs partenaires externes, au premier rang desquels, les banques : leurs partenaires bancaires sont souvent ceux qui détectent les premiers une anomalie. Il faut donc, quand un banquier appelle, l'écouter, il faut avoir le dispositif qui permet d'enregistrer ce que le banquier transmet au corporate, parce que c'est une des clés de l'identification d'un problème.
Le commissaire aux comptes peut, lui aussi, aider, dans l'exercice de ses diligences, à identifier un certain nombre d'anomalies ou de comportements risqués.
Et enfin, cela peut choquer, mais je pense que la veille concurrentielle est importante. Savoir ce que le concurrent dit de vous va peut-être, dans certains cas, vous permettre de détecter une anomalie dans votre département commercial ou dans les pratiques de vos vendeurs.

Dans les plus grosses entreprises, on peut mettre en place une structure beaucoup plus complète, qui prendra des formes différentes, mais, on l'a vu, il n'y a pas une meilleure pratique qui se détache.
Un point clé est d'arriver à concilier ce qui relève du traitement régulier d'informations, de ce qui nécessite des investigations complémentaires à partir de données croisées. Il ne faut pas se contenter d'un département qui traite l'information, il faut aussi aller la chercher. Il faut aussi savoir mener une investigation complémentaire, lorsque les preuves ou les suspicions sont fortes. C'est cette agilité qui évite de se heurter à l'écueil de la volumétrie.

Noël PONS

Mais que vient faire l'audit interne dans cette galère ? Quel est son positionnement ?

Jean-François SAUTIN

Je suis aujourd'hui convaincu que l'audit n'a pas vocation à être un détecteur de fraude. Il ne sait pas et il ne peut pas, sauf cas très rares, par exemple si l'on a dans son équipe un *Certified Fraud Examiner*. A la limite, l'audit peut même être contreproductif.

Pourtant, la nature même du travail de l'auditeur fait qu'il est, plus que d'autres, très proche de la fraude. C'est donc une préoccupation en filigrane de toute action d'audit, et l'auditeur doit analyser, à partir des risques, les conséquences potentielles de la fraude. L'auditeur doit être sensibilisé à l'environnement de fraude.
Lorsque, au cours d'une mission d'audit, on a une suspicion de fraude, on enclenche le plan B, on se mobilise et on creuse. En général, les auditeurs font cela en liaison immédiate avec le centre pour convenir de la façon d'agir dans les meilleures conditions possibles.
Dans nos formations annuelles, nos séminaires de départements, etc., la sensibilisation à la fraude est un des sujets que nous abordons régulièrement, compte tenu de la rotation permanente des auditeurs.
Voilà ce que je veux dire : l'auditeur n'est pas un détecteur de fraude ; ce n'est pas son objectif premier ; mais il est certain que l'audit ne se désintéresse pas du problème de la fraude.

En tant que patron du département d'audit, et en liaison étroite avec la direction juridique, je tiens ce que nous appelons un registre des fraudes. La remontée systématique des fraudes se fait vers la direction juridique et les directions de l'audit, et c'est la direction de l'audit qui garde un registre de tous les cas connus.
Cela fait un peu office de *KPI*. C'est une base de travail qui nous permet de mieux prendre la température du groupe pour ce qui concerne la fraude. Le registre des fraudes est par ailleurs partagé avec le comité exécutif du groupe et le comité d'audit de Lafarge, à chaque clôture des comptes.

Pour les cas de fraude plutôt significatifs, nous diligentons une mission d'audit dans les six mois qui suivent, pour nous assurer que l'analyse a été bien faite, que les dispositions prises nous paraissent adéquates, pour satisfaire le groupe, et faire savoir que la leçon a été retenue.

Frédéric GEOFFROY

Le mandat de l'audit est défini par des directives internes, à la Société générale, comme dans toutes les sociétés. Ces directives internes sont fondées sur des textes réglementaires, principalement le règlement 97-02 pour le secteur bancaire.
Aux termes de ces directives, il n'y a pas de responsabilité de premier niveau pour l'audit dans la détection de la fraude. Je reprendrai donc exactement ce qu'a dit Jean-François : l'audit n'a pas vocation à être détecteur de fraude, d'autant plus que, comme je l'ai indiqué précédemment, la plupart des banques mettent aujourd'hui en place des équipes de prévention et détection de la fraude.

Le rôle de l'audit n'en est pas moins important dans ce domaine, à toutes les étapes de son action. Il s'agit d'abord d'intégrer, de manière explicite, le risque de fraude dans la procédure de *risk assessment* qui conduit à la définition du plan d'audit de l'année suivante. La fraude est un facteur de risque essentiel, il faut l'identifier en tant que tel, identifier les entités concernées par ce risque et, si possible, déterminer la probabilité de risque et l'impact sur l'activité et les résultats de l'entité concernée.
Il faut ensuite intégrer, de manière systématique, des contrôles anti fraude dans le cadre des vérifications courantes. Je citerai par exemple, en ce qui concerne la banque, les contrôles qui figuraient dans le rapport Lagarde de 2008 : la surveillance des encours nominaux, les flux de trésorerie, les annulations/modifications, la réconciliation des positions, la surveillance des confirmations et l'exploitation des demandes d'information des autorités de marché. Cela me semble être le minimum quand on vérifie, quand on audite une activité de marché.

Lorsque, au cours d'une vérification, on détecte une faiblesse qui peut constituer un risque de fraude, il faut alerter rapidement sur ce dysfonctionnement susceptible de favoriser la fraude. Il faut le faire avant la fin de la mission. L'alerte doit remonter directement aux opérationnels concernés et de manière assez restreinte. Ce genre de mémo d'alerte n'a évidemment pas les mêmes destinataires que le rapport final.
En outre, il faut être capable de transversaliser rapidement. Un dysfonctionnement a été noté dans un service, sur une application informatique, un problème d'accès à des informations confidentielles, il faut immédiatement vérifier que cette faiblesse, ce dysfonctionnement ne se retrouvent pas dans d'autres entités, sur d'autres activités ou sur d'autres applications informatiques.
Enfin, il faut être en mesure de suivre activement la mise en place rapide des recommandations, surtout quand elles concernent des mesures de remédiation à prendre pour prévenir le risque de fraude.

Le rôle de l'audit, lorsqu'une fraude est détectée, est de rédiger un rapport en responsabilité pour établir les faits. Ce rapport en responsabilité ne propose pas de sanction, mais il est transmis à un comité qui réunit la hiérarchie, un certain nombre de personnes des relations humaines, et l'audit évidemment. C'est ce comité qui décidera de la sanction.

Dans la plupart des établissements, maintenant, toutes les missions spéciales sur les fraudes, tous les cas de fraude ou même les soupçons de fraude sont remontés à la direction générale et, pour les cas les plus graves, au comité des comptes.
C'est la procédure normale, classique. Je crois que l'audit doit également être en mesure d'effectuer des vérifications ciblées, courtes et inopinées en dehors des vérifications qui ressortent du plan d'audit. L'élément de surprise n'est pas à négliger.
Encore une fois, il faut généraliser l'utilisation d'extracteurs de données, de *data mining*, surtout quand on doit se pencher sur des fichiers complexes et volumineux. Et il faut systématiser les

approches intégrées audit métiers, audit systèmes d'information, pour être sûr de couvrir l'ensemble du champ.

Enfin, pour revenir sur un élément qu'a indiqué Mariano, je crois qu'il faut que l'audit travaille de plus en plus avec les autres départements de la banque et avec les commissaires aux comptes. Il est très important de disposer d'un maximum d'informations, et donc de réunir les informations des provenances les plus diverses.

Noël PONS

Jean-François va nous expliquer comment l'audit intervient en coordination avec d'autres structures.

Jean-François SAUTIN

Nous sommes en interface très active avec plusieurs départements. Le contrôle interne est organisé indépendamment de l'audit : le contrôle interne rapporte à la direction juridique, l'audit rapporte au CEO.
Le contrôle interne est un des vecteurs de maturation d'une approche de la fraude beaucoup plus robuste, puisque c'est lui qui travaille avec les entités opérationnelles pour mettre en place les contrôles, les animer, les vérifier, pour s'assurer que les autotests sont satisfaisants, etc.
L'audit vient en appui de ce dispositif pour s'assurer qu'il fonctionne. Il est également en relation avec le département juridique, entre autres pour la réflexion sur l'efficacité de notre système de lutte contre la fraude.
Même si je vous ai dit que l'audit n'était pas détecteur de fraude, il est certain qu'il est très impliqué dans les discussions, non seulement autour de la fraude, mais aussi du code de conduite des affaires en général, pour réfléchir à l'amélioration continue de ces systèmes. On ne peut pas tout faire tout de suite, mais il faut aller dans le sens d'une amélioration continue de notre dispositif et surtout d'une adaptabilité permanente, parce que le monde change, les systèmes changent, et il faut se battre sur le bon terrain.

Noël PONS

Maintenant, je voudrais demander à Mariano quels sont les dispositifs de suivi et de reporting qui permettent de lutter efficacement contre la fraude.

Mariano MARCOS

Je crois que la clé est le traitement de l'information. Deux types d'informations doivent être transmis au *top management*. D'une part, une analyse détaillée des fraudes commises, des mesures correctives mises en œuvre, et la remise en cause du dispositif (formation, structure, organisation) qui a permis l'occurrence de la fraude. Cette analyse doit bien sûr être traitée en petit comité, pour ne pas ébruiter les faiblesses identifiées. D'autre part, la définition d'un certain nombre d'indicateurs qui donneront la température sur le risque de fraude au sens large, pour le groupe. Il faut déterminer, selon l'activité et les zones à risque, un certain nombre d'indicateurs qui seront régulièrement remontés, qui permettront de porter une appréciation sur une détérioration ou une amélioration d'une faiblesse induisant un risque de fraude.
On a parlé, sur les activités de marchés, d'un certain nombre d'éléments : confirmation, annulation de deal, opération à départ décalé, etc. Je pense que d'autres opérations peuvent permettre de porter une appréciation sur la discipline ou sur une propension potentielle à frauder. Avec certains indicateurs, on peut juger de la qualité de l'amélioration ou non de la gestion du risque de fraude.

Il faut utiliser toutes les informations autour de la fraude et de la gestion du risque de fraude dans toutes les communications business. Une des bonnes pratiques consiste, dans chaque réunion business, à consacrer un moment au risque de fraude, à l'analyse d'une fraude qui a été commise, soit dans l'entreprise, soit chez un concurrent, pour en discuter, la décortiquer, dire comment on peut l'identifier, et montrer ainsi aux collaborateurs que l'entreprise prête une grande attention à cette problématique. Quelles que soient les contraintes de croissance de chiffre d'affaires, quand on a des objectifs ambitieux, on laisse une place à la communication qui aide beaucoup ceux qui travaillent sur la gestion du risque de fraude ; cela leur permet d'apporter de la valeur dans l'entreprise, ce qui est aujourd'hui fondamental.

Hélène PLOIX

Un reporting me paraît extrêmement efficace, le reporting de l'audit interne au comité d'audit. Dans un certain nombre de conseils que je connais, les membres du comité d'audit reçoivent soit tous les rapports d'audit, si c'est une petite entreprise, soit les synthèses de tous les rapports d'audit. Et le fait que, à chaque comité d'audit, un dialogue s'instaure entre les membres du comité d'audit et l'audit interne, et que les responsables d'unités sachent que les conclusions des audits menés dans leur structure remontent au comité d'audit, a, selon moi, une certaine force de persuasion. Et je recommande vivement à tous d'essayer de créer ce dialogue entre l'audit interne et le comité d'audit.

Noël PONS

Mariano, le *Shared Service Center*, le service partagé, favorise-t-il la fraude ?

Mariano MARCOS

On voit se développer de plus en plus les centres de services partagés au sein des grands groupes qui traitent énormément de flux, comme les banques ou les sociétés d'investissement ou d'assurance. Différents paramètres font qu'il y a un risque de fraude accru sur certaines opérations.
Dans ces *Shared Services Centers*, les personnes ont un sentiment d'appartenance au groupe moins fort que celles qui sont sur le site. Si elles traitent par exemple en centrale l'ensemble des paiements fournisseurs du groupe au niveau mondial, elles vont se sentir moins concernées par le business ; ce sont moins des collaborateurs que des « mercenaires », qui vont d'un *Services Center* à un autre, et qui peuvent être sensibles aux failles qu'ils vont détecter dans leur travail.
Dans les *Shared Services Centers*, la volumétrie, très importante, a un effet de dilution des tentatives de fraude dans l'ensemble des flux, ce qui rend plus difficile l'identification d'une fraude commise sur des petits montants.
Il faut se prémunir contre une idée reçue : ce qui est bon pour le centre de services partagés, est bon pour le groupe. On discute rarement une décision prise par quelqu'un qui travaille dans le centre de services partagés, alors que cette décision peut, dans certains cas, être sujette à caution, et justifier une réaction voire une alerte.
A l'égard de ces nouveaux risques, il est essentiel de réorienter l'épicentre du dispositif de gestion du risque de fraude. Il faut positionner ce dispositif à côté ou sur le site des centres de services partagés, ou, à tout le moins, disposer d'une antenne solide, et mettre en place un certain nombre d'indicateurs, un dispositif de surveillance adapté.
Il faut aussi prendre en compte d'autres aspects comme les échanges, le traitement des flux entre les entités et le centre de services partagés. On va constater un accroissement de circuits d'information, des envois et des retours d'informations. Il faut s'assurer que ce dispositif, techniquement parlant, est robuste, qu'il ne peut pas être détourné. C'est un des axes de travail majeurs dans la recherche du risque de fraude.

Et il faut bien sûr, en parallèle, revoir entièrement l'organisation et les programmes d'intervention de l'audit interne. Lorsque l'on met en place cette structure, l'audit interne verra un certain nombre de risques disparaître dans les entités, et apparaître, de manière peut-être plus prégnante, dans les centres de services partagés.

Noël PONS

Une dernière question : on a traité l'information interne, mais comment traite-t-on les informations qui viennent de tiers ?

Mariano MARCOS

L'identification d'une fraude vient souvent d'une information d'un tiers. Il faut donc être capable de la traiter. Des consultants qui travaillent sur un projet, chez vous, peuvent s'étonner d'un lien hiérarchique, d'un type d'organisation, de certaines habilitations sur des systèmes ; tous ces points méritent d'être éclaircis.
Il y a aussi les réunions dans les organisations professionnelles, les clubs, les associations, les cercles où l'on discute, où l'on échange entre pairs, sur les meilleures pratiques. Il y a beaucoup de valeur dans ces échanges d'informations.
Sur les marchés financiers, ceux qui parlent le plus, ce sont les courtiers. Il faut profiter des bavardages des courtiers, qui contiennent 10 % d'informations très intéressantes, très précieuses. Si le manager de l'équipe n'est pas régulièrement à l'écoute des courtiers ou s'il perd le fil avec le business, le terrain, il se coupe d'un certain nombre d'informations critiques, et ne pourra pas réagir de façon adéquate, et en temps voulu.

Noël PONS

Et maintenant, la question essentielle : qu'attendent le président et les administrateurs comme informations ?

Hélène PLOIX

Le président et les administrateurs attendent un certain nombre d'informations. Ils attendent d'abord du comité d'audit que celui-ci leur dise, de façon très claire, quels sont les cas de fraude, comment ils ont été traités et si les conclusions en ont été bien tirées. Ils attendent aussi de savoir, au travers du travail régulier du comité d'audit avec l'audit interne, avec l'audit externe, avec – quand il existe – le contrôle interne, si ces discussions approfondies font apparaître des lacunes ou si, au contraire, les processus sont bien maîtrisés ; et, s'il y a des lacunes, ce qui a été mis en œuvre pour y remédier.
Il y a donc une très grande confiance, si je puis dire, entre le conseil d'administration et le comité d'audit : ce qui doit être vu est vu, et ce qui est important est rapporté au conseil d'administration.
De même, il est important que le comité d'éthique soit totalement transparent vis-à-vis du conseil, et qu'il explique les procédures et tous les moyens mis en place pour s'assurer d'une très bonne *compliance* dans l'organisation à l'égard des valeurs de l'entreprise.
En fait, le président, dans la plupart des sociétés, étant président-directeur général, il est totalement opérationnel. C'est plutôt le conseil qui veut la garantie que les contrôles fonctionnent de façon efficace, et que l'entreprise se comporte de la façon dont le conseil et son président souhaitent qu'elle se comporte.

Tout cela implique un climat de grande confiance, mais aussi une totale transparence entre les uns et les autres, et que chaque comité aille au fond des choses et pose les bonnes questions à tous les échelons de l'organisation.

Frédéric GEOFFROY

La commission bancaire prévoit expressément que le responsable du contrôle périodique doit pouvoir informer directement et de sa propre initiative le comité d'audit, sur des enquêtes en cours, des conclusions qui en sont tirées et, éventuellement, de l'absence d'exécution des mesures correctives qui ont été décidées. Le responsable du contrôle périodique doit avoir accès directement au comité d'audit, et ceci très régulièrement.

En ce qui concerne la fraude, le règlement 97-02 qui a été plusieurs fois modifié depuis 1997, stipule que les systèmes d'analyse et de mesure des risques doivent prévoir les critères et seuils permettant d'identifier comme significatifs les incidents révélés par les procédures de contrôle interne. Est réputée comme significative toute fraude entraînant une perte ou un gain d'un montant brut dépassant 0,5 % des fonds propres de base. Ce montant ne peut être inférieur à 10 000 euros.
Les incidents doivent être portés sans délai à la connaissance de l'organe délibérant et de l'organe exécutif.
La commission bancaire doit avoir connaissance de ces critères. Elle doit pouvoir vérifier la pertinence des critères et des seuils de significativité. Elle peut en demander la modification si elle estime qu'ils ont été mal fixés.
Enfin, l'organe exécutif est chargé de transmettre sans délai à la commission bancaire les incidents significatifs au regard des critères définis.
Les règles sont donc très précises et ne laissent aucune marge d'appréciation.

Il en va de même pour la plupart des régulateurs dans la plupart des pays, notamment les pays anglo-saxons. Il en va ainsi au Royaume-Uni, depuis le *Fraud Act* de 2006. C'est un document très détaillé qui insiste particulièrement – et c'est intéressant – sur le modus operandi de la fraude.
Pour les Anglais, c'est le modus operandi qui définit la fraude, beaucoup plus que l'aspect gain, direct ou indirect, pour le fraudeur. Le modus operandi peut être, est souvent, est toujours dissimulation, représentation mensongère, usurpation de fonction, manipulation d'informations.
La FSA ne donne pas de seuil. Tout incident significatif doit être immédiatement notifié, même le simple soupçon de fraude. Non seulement il convient de notifier la fraude ou le soupçon de fraude, mais il convient également de transmettre à la FSA les éléments qui lui permettent d'en apprécier rapidement l'impact sur les comptes et éventuellement sur la réputation de l'établissement concerné, sur les clients de l'établissement concerné, et sur les autres établissements ou les partenaires financiers de cet établissement. C'est une notification très détaillée.
Le *Fraud Act* prévoit les sanctions. Ces sanctions sont évidemment lourdes pour le fraudeur, mais elles sont également lourdes pour l'employé qui n'a pas signalé un cas de fraude, avec un maximum de cinq années d'emprisonnement ; lourdes aussi pour le *tipping-off*, c'est-à-dire l'employé qui indiquerait à un autre employé suspecté de fraude qu'une enquête est en cours, délit également passible de la prison en Angleterre. Depuis trois ans, tous les régulateurs ont durci très fortement les sanctions et les dispositifs concernant la fraude.

QUESTIONS/REPONSES

Noël PONS

Avez-vous des questions à poser aux intervenants ?

Jacques RENARD

Je souhaiterais faire deux remarques.

La première est que je suis tout à fait d'accord avec Mme Ploix quant au problème de l'exemplarité, qui est à coup sûr un point de touche essentiel en matière de lutte contre la fraude.
En revanche, je ne pense pas que les méthodes de *wistleblowing*, finalement peu adaptées à nos cultures, changent grand-chose au système, et les exemples récents nous montrent qu'elles n'ont pas apporté beaucoup d'efficacité dans ce domaine. J'ai moi-même pu constater, dans la vie professionnelle, à quel point, dans nos pays, elles étaient plutôt le réceptacle d'opinions personnelles souvent mal placées que véritablement des facteurs d'efficacité.
Mais je rejoins tout à fait ce que disent M. Sautin et M. Geoffroy, pour souligner que la politique de reporting, dans le domaine des moyens, est certainement un élément essentiel. J'ai moi-même travaillé dans une entreprise qui avait organisé, au niveau mondial, le système suivant : chaque fois qu'une fraude se produisait dans un point quelconque de la planète, elle était diffusée anonymement à tous les acteurs de l'entreprise dans le monde, avec – et c'était évidemment le plus important – l'explication de la façon dont les défaillances de contrôle interne avaient permis la réalisation de cette fraude. L'analyse causale est donc, de ce point de vue, quelque chose d'essentiel.

Deuxième remarque. Je ne suis pas tout à fait d'accord avec M. Geoffroy. Je suis bien d'accord avec lui, sur le fait que le seuil de signification, pour les auditeurs externes qui doivent certifier un résultat, est très important. Mais ce seuil de signification, en ce qui concerne les problèmes de fraude et singulièrement l'audit interne, est, si j'ose dire, sans signification, pour la simple raison qu'un seuil de signification insignifiant, la mise en cause d'une somme insignifiante peut receler une faiblesse de contrôle interne majeure qui sera, demain ou après-demain, à l'origine de problèmes essentiels.

Frédéric GEOFFROY

En fait, je crois que nous sommes tout à fait d'accord. Le seuil de signification que j'ai indiqué est celui qui est stipulé par la commission bancaire dans le 97-02, seuil au-dessus duquel il est obligatoire de rapporter à l'organe exécutif, à l'organe délibérant et à la commission bancaire. Dans la pratique, je suis tout à fait d'accord avec vous, il est essentiel de remonter tous les cas de fraude, et de les analyser. Et la direction générale doit avoir connaissance de tous les cas de fraude.

Jean-François SAUTIN

Je suis d'accord avec vous, M. Renard, et j'ai appris de mes auditeurs que les réconciliations bancaires devaient être exactes au centime près. En tant qu'ingénieur, je n'avais pas nécessairement ce même réflexe, au départ.

Frédéric GEOFFROY

Jean-Baptiste Giros est inspecteur principal à la Société Générale. Il a conduit l'enquête sur la fraude Kerviel, et il va nous dire quels enseignements on peut tirer de cette affaire.

QUELS ENSEIGNEMENTS PEUT-ON TIRER DE L'AFFAIRE KERVIEL ? PAR JEAN-BAPTISTE GIROS

Inspecteur principal, Groupe Société Générale

Je ne vais pas vous raconter comment la Société Générale a réagi et a modifié l'ensemble de ses comportements à la suite de l'affaire Kerviel. Ce serait long et ce n'est pas vraiment l'objet de mon intervention. Je vais rappeler brièvement les mécanismes de la fraude, tels que nous les avons identifiés dans le cadre de notre mission d'investigation interne. Je reviendrai ensuite sur les spécificités de l'intervention d'une inspection générale ou d'un audit interne sur une fraude d'une telle ampleur. Enfin, j'évoquerai quelques pistes sur les grands enseignements que l'on peut tirer d'une telle fraude à l'égard du contrôle périodique.

1. Les principaux mécanismes de la fraude

Je sais que je vais certainement échouer à convaincre certains d'entre vous, mais cette fraude a été possible, et elle a été possible sans la complicité du *top management* de la banque. Je peux vous l'assurer.

Kerviel prenait des positions réelles sur les marchés. Il achetait 100 actions, puis il entrait dans les systèmes des transactions inverses, donc -100 pour que, dans les systèmes de la Société générale, n'apparaisse pas de position ; dans nos systèmes, les positions qu'il prenait étaient masquées.
Comment faisait-il ? Il y a un certain nombre de possibilités d'entrer dans les systèmes des transactions avant qu'il y ait confirmation et donc exécution réelle de la transaction. Dans un certain nombre de marchés, il est possible de contractualiser une transaction avant l'exécution réelle, c'est ce que l'on appelle des transactions à départ différé. Ce sont des pratiques de place. Un lundi, vous passez un accord avec un opérateur de marché pour un achat de *futures* en fin de semaine, et c'est seulement en fin de semaine, parce qu'il n'y a qu'une journée dans la semaine où il peut se passer telle ou telle transaction, que la transaction s'effectue réellement : confirmation, échange de papier montrant que la transaction a bien eu lieu, et échange de flux.
Néanmoins, dans les systèmes de risques et de contrôle des risques de la banque, on choisit d'intégrer cette transaction dès le moment où on passe l'accord avec l'opérateur de marché, pour être bien conscient que l'on a ces risques dans le bilan de la banque, par précaution, puisqu'à partir du moment où on passe l'accord avec un opérateur de marché, on est engagé et on doit donc, à la fin de la semaine, quels que soient les événements qui ont pu se produire entre-temps, délivrer les titres ou délivrer le cash, en fonction du type d'opération.
Selon les types d'opération, les délais peuvent varier de quatre/cinq jours à deux ou trois semaines. Kerviel entrait donc tout simplement les fausses transactions et, la veille du jour où il devait y avoir réalisation effective de la transaction, il annulait l'opération et il choisissait soit de réécrire une opération telle que je viens de la décrire, soit d'utiliser une autre technique.
Les autres techniques : cela pouvait être la réalisation de fausses transactions avec des filiales du groupe Société générale ; les transactions internes entre deux filiales de la Société générale, comme c'est le cas dans beaucoup de banques, ne donnent pas lieu à confirmation immédiate mais seulement en fin de mois : cela lui donnait un peu de temps pour passer d'une technique à une autre, pour créer une autre transaction fictive.
Il montait donc une position réelle et, de l'autre côté, il avait une position exactement inverse irréelle qu'il remontait tous les trois/quatre jours, toutes les deux ou trois semaines, en fonction des nécessités du timing de la réalisation effective de l'opération qui allait mettre en exergue le fait que l'opération était fictive.
On a dénombré une petite dizaine de types de techniques de dissimulation d'une transaction fictive, et les produits sur lesquels il a réalisé ses prises de position étaient également de l'ordre de la

dizaine. Donc, si l'on croise les deux techniques, types de produits et techniques de dissimulation, on obtient entre 80 et 100 techniques de dissimulation, ce qui lui permettait de jongler entre ces différentes techniques pour ne pas aviver les suspicions. Ce qui explique aussi pourquoi les contrôleurs, les opérateurs de marché qui contrôlent tous les jours les activités des *traders*, n'ont pas repéré de comportement anormal, c'est que, comme il avait à sa disposition environ 80/100 techniques, il n'avait jamais en face de lui, plus de deux fois le même opérateur, et aucun des opérateurs interrogés ne comptait Kerviel parmi les principaux *traders* auxquels il avait affaire.
A partir de toutes les investigations, on a réussi à démontrer qu'il avait pu accumuler une position d'environ 30 milliards sur l'ensemble de l'année 2007, qui lui avait fait gagner 1,5 milliard. Il avait remonté une position à partir de janvier 2008, d'une cinquantaine de milliards d'euros, qui lui avait perdre 6,4 milliards : 6,4 milliards moins 1,5 milliard, cela fait bien 4,9 milliards de perte.

Sur les motivations et éventuelles complicités, on n'a pas trouvé d'indice de détournement. Les 4,9 milliards ne sont pas dans une valise dans l'appartement de Jérôme Kerviel ni sur un compte en banque en Suisse ou aux Bermudes. Ils ont été perdus sur le marché par la Société Générale.
Toutefois, lorsqu'il créait ses positions fictives, souvent, au lieu de faire +100/-100, il faisait +100/-99,9, pour réaliser un petit gain et le prendre dans son P&L officiel, ce qui lui permettait de pouvoir prétendre à un bonus, à une rémunération variable supplémentaire, et peut-être à une promotion.

Sur l'identification d'indices d'une complicité interne, je ne reviens pas sur le sujet, parce que je ne peux pas vous en dire beaucoup plus, sinon ce qu'il y a dans le rapport, c'est-à-dire que nous avons repéré des indices de complicité de la part de son assistant *trader*, qui ont été étudiés par la justice et qui ont abouti à un non-lieu. Nous pensons que l'assistant *trader* avait au moins conscience de ce qui se passait. Il n'a pas été forcément acteur de ce qui s'est fait. Maintenant, en dehors de cet assistant *trader*, on a analysé le cas de la plupart des personnes qui entouraient Kerviel jusqu'au plus haut niveau de la banque et aucune n'avait connaissance de ses agissements.

En revanche, Kerviel avait un réseau interne de relations personnelles étendu, ce qui lui a certainement permis, dans un certain nombre de cas, de contourner les contrôles.

En étudiant les différents mécanismes, on comprend un peu mieux comment Kerviel a pu contourner les contrôles permanents du *middle* et du *back office*. Ce qui, en revanche, a été plus long à comprendre, c'est comment il a pu échapper à la vigilance de ses supérieurs directs, qui étaient assis à ses côtés, pendant tous ces mois.
Il y a eu de fait un concours de circonstances et un certain nombre de défaillances. Le concours de circonstances est que le *desk* a été créé fin 2006, et que le responsable a démissionné en 2007, et n'a pas été remplacé au pied levé. Pendant trois mois, Jérôme Kerviel n'a pas eu formellement de N+1. Au même moment, le N+2 de Kerviel, qui aurait dû compenser l'absence de N+1, a eu un certain nombre de sujets brûlants à traiter, opérationnels, business, et a donc relâché sa supervision sur Kerviel. Et, l'on voit que les prises de position massives ont commencé en février 2007.
Le nouveau N+1 est arrivé en mai 2007. C'était un ingénieur qui connaissait les produits structurés. Il avait passé trois ou quatre ans en Asie. Il n'avait aucune expérience en matière de supervision de desk de *trading*. Il lui a donc fallu quelques semaines pour se mettre dans le coup. Kerviel était le *trader* le plus expérimenté. Et le manager a fait preuve de laxisme dans sa supervision, privilégiant un suivi, non pas transaction par transaction, mais en delta. Il voyait +100 -100 = 0, donc pas de position. Or on demande à un manager de *trading* – et c'est bien entendu le moins que l'on puisse lui demander – à la fin de la journée, d'expliquer le P&L de ses différents *traders*, notamment en listant transaction par transaction pour comprendre, en termes de *business model*, d'où viennent les gains annoncés.
Ce manager, au bout de trois/quatre mois, n'avait toujours pas les bons réflexes et s'est montré défaillant dans sa supervision. Il a subi des remontrances de son N+2, deux semaines avant la détection de la fraude. Il y a donc eu là un concours de circonstances extrêmement mal géré par un N+2 pris dans des priorités autres et un N+1 défaillant quand il a pris son poste.

S'agissant des fonctions de support, ce qui nous a beaucoup surpris c'est que l'on pensait découvrir que plusieurs opérateurs avaient failli et que les contrôles n'avaient pas été réalisés, que les fichiers d'alerte n'avaient pas été lus, que le *trader* n'avait pas été questionné. Or, dans toutes les alertes déclenchées, les opérateurs ont fait leur travail ; il n'y a pas eu d'opérateur défaillant à proprement parler.
En revanche, deux lacunes sont apparues. Premièrement, il manquait de transversalité dans les contrôles. Il y a eu une ou deux alertes par opérateur sur une année, ce qui est très peu ; sur les marchés, il y a tellement de transactions qu'un *trader* que l'on voit trois fois dans l'année ou même dans le semestre, ce n'est pas un *trader* qui pose problème. Il aurait fallu un certain nombre de contrôles transversaux permettant de profiler les *traders* à risque, et nous ne les avions pas. Il n'y avait pas cette instance permettant de croiser les différentes alertes, ce qui aurait évidemment fait ressortir le *trader* Kerviel.
Deuxièmement, les opérateurs réalisaient leurs contrôles formellement, mais n'approfondissaient pas suffisamment les dires du *front officer*. Kerviel répondait en général par des mensonges, ou écartait le problème en abordant un autre sujet, ou utilisait des termes techniques qui pouvaient faire croire à l'opérateur que la situation était sous contrôle alors qu'elle ne l'était pas du tout. Les opérateurs se sont également laissé abuser par des faux mails montés par Kerviel.
Parmi les contrôles qui manquaient, le contrôle sur les transactions annulées nous aurait permis de comprendre la technique de Kerviel qui consistait, *in fine*, à entrer une transaction fictive, à l'annuler pour en refaire une autre et gagner un peu de temps. Si nous avions eu un contrôle sur les transactions annulées, on aurait vu ressortir Kerviel devant tout le monde cent fois ou mille fois. Malheureusement, ce contrôle n'existait pas.

2. Le rôle du contrôle périodique dans les investigations

Comment l'intervention de l'inspection sur le sujet s'est-elle déroulée ?

Une gouvernance spécifique, adaptée aux enjeux et aux attentes externes a été mise en place. La fraude était tellement massive et l'attente de la communauté financière et des médias était telle que le conseil d'administration a décidé de rattacher l'équipe que je pilotais, non pas au PDG de la banque de l'époque, mais à un comité spécial d'administrateurs indépendants, dirigé par Jean-Martin Folz, qui nous donnait, sur le plan formel, une totale indépendance vis-à-vis du *top management* de la banque. Je faisais régulièrement des points avec ce groupe d'administrateurs.
Nous étions également suivis et coachés, quotidiennement, par deux membres du comité exécutif. En outre, le cabinet de conseil externe, PricewaterhouseCoopers intervenait en tant que *peer review*. Il faut dire que la décision de confier à l'inspection générale, c'est-à-dire au contrôle périodique interne, la conduite des investigations a fait débat. En effet, historiquement, toutes les grandes fraudes sont normalement traitées par des cabinets externes, tout simplement par souci d'indépendance. Mais, dans l'affaire Kerviel, le conseil d'administration de la banque a jugé que les attentes étaient telles que les résultats devaient être obtenus extrêmement rapidement, et que le temps qu'il aurait fallu à un cabinet externe pour se familiariser avec les systèmes d'information internes, les équipes, les différents départements impliqués, aurait été trop important.
C'est pourquoi l'inspection générale a été mandatée. Le cabinet externe comprenait une dizaine de personnes ; nous mêmes étions une quarantaine. Pendant trois mois, un membre du cabinet m'a suivi partout, en réunion, dans mon bureau, pour établir le constat que l'avis donné par l'inspection était indépendant et basé sur des analyses cohérentes et pertinentes.
Ce dispositif a donné satisfaction à la communauté financière et aux régulateurs.

Notre lettre de mission était extrêmement précise et réaliste. Je ne vous souhaite pas de connaître notre expérience, mais si vous devez intervenir sur une fraude massive, il faut éviter deux écueils.
Premier écueil : on vous demande de chercher tous les risques de fraudes à l'intérieur de l'établissement, et de garantir que tous les risques sont couverts, et qu'une telle fraude ne peut pas se reproduire. C'est évidemment un champ beaucoup trop large, et il faut freiner les dirigeants dans leur emballement.

Deuxième écueil : il ne faut pas se laisser instrumentaliser.
On a donc passé un certain temps à définir le périmètre de la mission, et l'on est parvenu à un bon compromis. Nous avions quatre objectifs : premièrement, détricoter les mécanismes de la fraude. Deuxièmement, analyser les éventuelles complicités et les motivations du *trader*. Troisièmement, identifier les dysfonctionnements. Quatrièmement, mener une série de contrôles visant à montrer qu'il n'y avait pas d'autres fraudes similaires ailleurs dans la banque. Mais là, il ne faut pas « se laisser embarquer » trop loin, car on risque de tomber sur le premier écueil dont nous avons parlé.

Il a fallu faire un compromis entre la totale indépendance des investigations, sur laquelle on a beaucoup insisté au début auprès de nos dirigeants – mais sur laquelle on n'a rien eu à redire, le principe en interne ayant été celui de la transparence totale, allant jusqu'à la publication sur Internet, et ailleurs, de notre rapport – et la participation à la gestion de la crise au niveau du groupe.
Il ne fallait pas que nous jouions contre notre camp. La transparence était bien entendu totale vis-à-vis de l'extérieur, mais également en interne : il n'était pas question, de notre part, de ne pas tenir au courant les instances dirigeantes de la banque de l'avancée de nos investigations.
La plus grosse partie de l'équipe était sur la réalisation des investigations ; des personnes faisaient le lien avec la gestion de crise au niveau du groupe ; d'autres, avec les commissaires aux comptes qui étaient, eux, plutôt anxieux, puisque la fraude a été détectée le 20 janvier 2008 et qu'ils devaient signer les comptes en mars. Une personne était en charge, à temps plein, de la relation avec la brigade financière et la justice. Il faut savoir que nous avons travaillé avec les policiers, main dans la main, et nous les tenions au courant au jour le jour de l'avancée de nos investigations. Deux personnes étaient en charge des relations avec la Commission bancaire, et en particulier les représentants de l'inspection générale de la Commission bancaire qui devaient rédiger leur propre rapport.

Dans une telle intervention, il faut bien entendu gérer la réalisation des investigations, des contrôles, des recherches, des analyses, mais il faut aussi gérer tout l'aspect gouvernance. D'où une mobilisation des moyens et une organisation en mode projet : comme je vous l'ai dit, nous étions une quarantaine sur la mission, c'est très différent d'une mission d'inspection, d'une mission d'audit classique. Pour mener les investigations, il faut à la fois se raccrocher à ce que l'on sait faire, retourner aux basiques, tout en s'adaptant et en tenant compte des délais extrêmement serrés, et donc organiser les travaux de manière un peu différente de d'habitude.
Nous avons dû rédiger un rapport intermédiaire. A l'audit comme à l'inspection, on n'aime pas beaucoup faire ce genre de choses, mais il fallait le faire car on ne pouvait pas demander aux media d'attendre quatre ou cinq semaines un premier papier de l'inspection générale de la Société générale ; c'était inenvisageable à l'époque.

En résumé, cette mission désagréable et compliquée, m'a beaucoup appris.

3. Les enseignements pour le dispositif de contrôle périodique

J'ai sélectionné quatre thèmes.

Avec l'affaire Kerviel et après les investigations internes, nous avons passé plusieurs mois – et on est toujours sur le sujet – à remettre en question nos méthodes de travail et à chercher la raison pour laquelle nous n'avions pas détecté cette fraude, nous-mêmes, le contrôle périodique. L'ensemble de la banque, et notamment les *front offices*, les *back offices* et *middle offices*, la direction des risques ont mené une réflexion identique.

L'identification des zones de risque. Le desk de Jérôme Kerviel était dans notre plan d'inspection pour le deuxième semestre 2008. Il était d'ailleurs également dans le plan d'audit de la banque de financement et d'investissement. Nous avions donc bien identifié la zone de risque, mais avions considéré qu'auditer une activité de moins de deux ans, était un peu prématuré. A posteriori, nous avons eu tort.

Cela nous a incités à revoir notre manière de réaliser notre *risk assessment* : dans certains cas, une activité, même si elle ne fonctionne que depuis six mois, mérite une intervention. Dans d'autres cas, au contraire, on peut attendre plus longtemps. Il faut être attentif à la création d'activités.
Nous avions été informés de la création du desk de Jérôme Kerviel, mais seulement plusieurs mois après. Là-dessus, nous avons modifié un certain nombre de points.

La conduite des travaux de détection des fraudes. Nous avons refondu toute notre méthodologie. Mais, surtout, nous avons insufflé un nouvel état d'esprit au sein des équipes, en leur faisant prendre conscience de la nécessité absolue d'aller au bout des investigations. Nous avons notamment insisté sur la manière de traiter ce que l'on appelle les constats de carence. Une mission d'audit a une durée définie, elle ne peut pas durer un an. Et c'est vrai qu'à la fin des missions, il peut arriver que l'audit ne dispose pas des documents lui permettant de conclure. Il établit alors un constat de carence. Nous nous sommes rendu compte qu'il y avait trop de constats de carence, et que ces constats peuvent être une façon, pour l'audité, de dissimuler une fraude.
Nous avons donc rappelé aux inspecteurs qu'il fallait éviter le plus possible les constats de carence, et qu'il fallait pousser au bout les investigations.

Le dimensionnement et l'adéquation qualitative des effectifs. Nous avons beaucoup réfléchi à la manière dont nos ressources étaient allouées aux différentes zones de risque. Nous avons constaté – mais dans toute organisation, c'est comme cela – une certaine pesanteur organisationnelle. De fait, les zones de risques bougent plus vite que les répartitions de ressources dans les différents départements. Nous sommes donc en train d'adapter notre organisation, afin d'être plus réactifs aux évolutions du *business* et de l'organisation des audités.

Le suivi des recommandations. Quand on fait la synthèse des différents rapports sur les départements en contact avec Kerviel, quelques mois avant la fraude, on constate que tant l'audit interne que l'inspection générale avaient soulevé un certain nombre de problèmes (la majorité des problèmes relevés après la fraude), mais que les préconisations et recommandations avaient mis trop de temps à être appliquées, et que nous n'avions pas suffisamment fait remonter au *top management* de la banque la nécessité d'intervenir auprès des différents supérieurs hiérarchiques pour que les préconisations soient davantage prises en compte.

Une nouvelle procédure de suivi des recommandations a donc été mise en place, qui fait davantage appel à l'escalade. Désormais, tous les deux mois, les principales préconisations non mises en œuvre remontent au comité exécutif du groupe, sont discutées, et donnent lieu à des injonctions d'application dans des délais extrêmement serrés, de quelques jours, voire moins.

Questions/Réponses

Question

De votre exposé, il ressort que les agissements de Jérôme Kerviel auraient pu être détectés par des mesures de contrôle assez basiques, comme la gestion des annulations et aussi, par exemple, le fait de ne pas prendre des vacances.
Cela ne montre-t-il pas que l'on a tendance à s'en remettre un peu trop, de nos jours, à des systèmes complexes – systèmes de gestion des risques, etc. – en négligeant un peu les opérations de contrôle un peu « primaires » ?

Jean-Baptiste GIROS

Je pense que l'on a besoin des deux. Pour être capable d'évaluer le risque de contrepartie sur une opération de marché, pour être capable d'évaluer le risque de marché sur une transaction structurée, on a besoin de modèles complexes.

En revanche, cela ne doit pas nous empêcher d'exercer des contrôles, que vous appelez plus basiques, sur les opérations annulées, sur les congés, et un certain nombre de comportements qui peuvent sembler suspects.
A ce sujet, a été créé par SGCIB une cellule anti fraude, au sein du contrôle permanent – hors contrôle périodique – censée agréger un certain nombre d'indicateurs, comme ceux que vous citez : non-prise de congés pendant plusieurs mois, nombre de deals annulés, taille des transactions réalisées, nombre d'alertes levées auprès d'un certain nombre d'opérateurs de marché, etc. Cette cellule antifraude, composée de quatre personnes, a pour vocation de réaliser ce type d'investigations complémentaires.

Question

Ma question porte sur le dimensionnement et l'adéquation quantitative des effectifs. Vous parliez d'une allocation des ressources en fonction des évolutions des zones de risque et donc d'une adaptation de l'organisation, avec une meilleure réactivité. Comment cela se traduit-il dans les faits ?

Jean-Baptiste GIROS

Cela se traduit concrètement par deux choses. Premièrement, par un renforcement des effectifs sur les parties que l'on considère comme les plus risquées. Il a fallu démontrer au *top management* de la banque que des effectifs supplémentaires étaient nécessaires pour couvrir telle ou telle zone de risque.
Deuxièmement, historiquement, à la Société générale, il y a l'inspection qui est rattachée à la direction générale, et il y a les audits qui sont rattachés aux pôles ou aux directions fonctionnelles concernées ; il en est ainsi de l'audit de la banque d'investissement et de financement. L'inspecteur général – et ce, depuis plusieurs années – exerce une autorité fonctionnelle sur l'ensemble des audits : il veille donc à la cohérence de l'ensemble du dispositif de contrôle périodique, inspection et audits compris, ce qui lui permet d'avoir une vision globale de tous les auditeurs du groupe et d'être capable, à l'issue du processus de *risk assessment* annuel, qui est un processus consolidé, de prioriser telle ou telle zone de risque.

Question

Merci pour cette réponse. Aujourd'hui, concernant le ratio auditeurs/audités, vous êtes à quelle hauteur ?

Jean-Baptiste GIROS

Aujourd'hui, on est à 0,8, me semble-t-il. Sachant que l'on considère par exemple que, s'agissant du Secrétariat général, on peut être à beaucoup moins, à 0,4 ou 0,5. En revanche, pour la banque de financement et d'investissement ou pour les activités de courtage, actions, etc., on est plus proche de 1, voire légèrement supérieur à 1.

Question

Quel est le rythme de rotation des équipes ? Le renouvellement des auditeurs ?

Frédéric GEOFFROY

En moyenne, quatre ans chez SGCIB, pour l'audit de la banque d'investissement, et deux ans de plus pour les superviseurs.

Jean-Baptiste GIROS

En ce qui concerne l'inspection générale, nous sommes environ 200, dont 160 personnes qui réalisent des missions. Les cursus durent six ans et demi. Nous disposons donc de professionnels de l'audit interne, qui ont une expérience suffisante pour conduire des missions complexes.

Question

A l'époque où le scandale a éclaté, si les positions de Jérôme Kerviel avaient fait gagner trois à cinq milliards à la banque, est-ce que les dispositifs en place auraient permis de constater que cet argent était lié à des pratiques dangereuses ? Et est-ce que, au moment de toucher son bonus, des contrôles auraient mis en valeur le fait que ces positions n'étaient pas réglementaires, ni conformes aux valeurs de la banque ?

Jean-Baptiste GIROS

Vous dites que, à un moment, cela nous a fait gagner beaucoup d'argent, c'est cela ?

Question

Non, je dis : si, à l'époque, au lieu de perdre de l'argent (4,9 milliards) la banque avait gagné de 3 à 5 milliards, bref, si les positions de Jérôme Kerviel s'étaient avérées fructueuses, est-ce que les dispositifs auraient permis de constater que ces positions étaient liées à des pratiques dangereuses et non réglementaires ? Et est-ce que, au moment de toucher son bonus, on aurait effectivement pu constater que ce bonus était lié à des pratiques non réglementaires, et est-ce que Jérôme Kerviel serait aujourd'hui poursuivi ?

Jean-Baptiste GIROS

La réponse est : oui. Bien évidemment, on aurait eu exactement les mêmes moyens d'identifier les mêmes dysfonctionnements. Il faut savoir que le début de la détection de la fraude a eu lieu le vendredi 18 janvier 2008, et que le samedi on a réussi à découvrir les mécanismes de la fraude – enfin, la plupart des mécanismes qui ont finalement été très vite identifiés – et que, jusqu'au dimanche matin, nous n'avions identifié que les positions de 2007, c'est-à-dire uniquement le gain de 8,5 milliards.
On avait donc tout de suite compris les mécanismes, on avait tout de suite compris que c'était une fraude et on avait évidemment d'ores et déjà décidé de licencier Jérôme Kerviel. Quand vous licenciez, vous ne distribuez évidemment pas de bonus. La sanction qui a été donnée à Kerviel n'est pas liée à la perte, elle n'est liée qu'au fait qu'il a contrevenu à son mandat, qu'il a dissimulé des positions, et qu'il s'est comporté de manière totalement antiprofessionnelle.

Question

Est-ce que, dans les enseignements que l'on peut tirer de l'affaire Kerviel, il y a un problème culturel ou un problème de communication et de positionnement entre les fonctions de contrôle et les *traders* ? Et si c'était le cas, y a-t-il des meilleures pratiques à recommander ou d'autres enseignements ?

Jean-Baptiste GIROS

Sur le plan culturel, il est clair que la Société générale, comme beaucoup de banques, ces dix dernières années, a vécu dans le culte du *front officer* innovant. L'opérateur de marché et le contrôleur vivaient à l'ombre de ce *front officer* innovant et, en quelque sorte, sacralisée.
Là-dessus, notre manière de voir les choses est d'abord d'essayer de faire des efforts dans le domaine du recrutement et de la rémunération de ces fonctions, et d'essayer de créer de la mobilité pour valoriser les postes de fonction de support. Mais je dirais que cela avait déjà commencé avant la fraude et c'est encore poursuivi.
Deuxième remarque : nos fonctions de support, que ce soient la direction des opérations, la direction des risques ou la direction financière et comptable, étaient déjà, avant la fraude, et le sont toujours, des fonctions hiérarchiquement indépendantes du *front office*. Sur le plan organisationnel, il n'y avait donc pas, en tout cas a priori, de réponse très forte à donner.

En revanche, ce dont on s'est rendu compte – et c'est un point important –, c'est la confusion qui régnait, dans la direction des opérations, entre les activités de production et les activités de contrôle. La majorité des opérateurs exerçaient des travaux incompatibles qui étaient d'une part, de produire et d'aider le *trader* dans ses tâches quotidiennes, d'autre part, d'exercer un rôle de contrôle théoriquement indépendant.
Prenant conscience de cette grave anomalie, SGCIB a lancé une réorganisation – c'est ce que l'on a appelé en interne le projet Evolution – et a créé un nouveau département ayant vocation à reconstituer le P&L quotidien en fin de journée ; c'est une tâche de contrôle, qui dépend de la direction financière et comptable, et qui n'exerce aucune activité au *front office*.

Frédéric GEOFFROY

Nous accueillons Mme Le Damany, associée dans le cabinet d'avocats Landwell & Associés. Elle va nous parler de la responsabilité de l'auditeur interne lors de la conduite d'une mission antifraude.

QUELLE EST LA RESPONSABILITE DE L'AUDITEUR INTERNE LORS DE LA CONDUITE D'UNE MISSION ANTI-FRAUDE ? PAR SYLVIE LE DAMANY

Avocat, Associée, en charge du contentieux et droit pénal des affaires, Landwell & Associés

Je rappellerai rapidement les textes fondamentaux sur le rôle et les responsabilités de l'auditeur interne, quelles sont en pratique ses responsabilités réelles, son exposition au risque de mise en jeu de sa responsabilité civile, voire pénale. J'évoquerai avec vous l'ordonnance du 8 décembre 2008, qui a fait évoluer le rôle et les responsabilités du conseil d'administration et du comité d'audit sur le suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques. Nous verrons ce que cela va changer dans la relation entre le comité d'audit et l'audit interne.

« L'audit est une activité indépendante et objective, qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. »
« Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. » Cette définition a été approuvée le 21 mars 2000 par le conseil d'administration de l'IFACI.

L'audit interne a plusieurs interlocuteurs au sein de l'entreprise. Il va aider la direction générale à réaliser ses objectifs, et aider le comité d'audit afin que celui-ci s'acquitte de ses responsabilités dans les domaines du risque, du contrôle interne, de la fraude et des enquêtes internes. Il y a un lien assez fort entre le comité d'audit et l'audit interne, notamment au regard de l'évolution législative récente (ordonnance du 8 décembre 2008).
Se pose une question de gouvernance : est-ce que les responsabilités des auditeurs internes vont évoluer en matière de contrôle, notamment de détection des fraudes ? Qui doit être le garant en matière de suivi des risques, de suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques ? Et finalement, qui est responsable en cas de carence dans le contrôle interne ?

Beaucoup de questions. Quels sont les textes de référence, concernant la fonction, la profession d'auditeur interne ?
Les normes professionnelles, qui ont d'ailleurs été revues le 1er janvier 2009 ; le code de déontologie ; la charte de l'audit interne qui est, à mon sens, un document très important, et qui doit être approuvé, rappelons-le, par le conseil d'administration. Ce document n'est pas destiné au seul usage des auditeurs internes, mais il est destiné également au conseil d'administration et au comité d'audit, ne serait-ce que pour rappeler le rôle des uns et des autres en matière d'audit interne. Il informe, et il sensibilise.

Quelle est la responsabilité de l'auditeur interne ? Les normes envisagent cette responsabilité, mais sans préciser son régime.
Selon la norme 1000, « la mission, les pouvoirs et les responsabilités de l'audit interne doivent être formellement définis dans une charte d'audit interne, être cohérents avec la définition de l'audit interne, le code de déontologie ainsi qu'avec les Normes. » C'est donc un document qui doit être revu périodiquement et soumis à l'approbation de la direction générale et du conseil.
La norme 1210 dit : « Les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. » Il y a donc des responsabilités individuelles et une responsabilité collective.
Norme 1220 : « Les auditeurs internes doivent apporter à leur travail » – comme tout professionnel – « la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne, raisonnablement averti et compétent. » Et, là, je le souligne, la conscience professionnelle n'implique pas l'infaillibilité. Personne n'est infaillible et le risque 0 n'existe pas.

Avant 2009, il est intéressant de rappeler la norme 1210 A2 qui dit que : « Les auditeurs internes doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation. » Mais, la norme le rappelle : « Toutefois, ils ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes. »
La modalité pratique d'application (MPA) 1210 A2-2 a été supprimée après la refonte des normes en janvier 2009. Que disait-elle ? Premièrement, que le management est responsable de la mise en place et du maintien d'un système efficace de contrôle à un coût raisonnable. Deuxièmement que l'auditeur interne est tenu d'exercer ses fonctions avec « conscience professionnelle », avec des connaissances suffisantes en matière de fraude ; et il doit en informer les organes compétents. Depuis le 1er janvier 2009, ces recommandations ont disparu.

En pratique, on peut dire que le rôle de l'auditeur interne dans la prévention de la fraude est d'évaluer les risques et les stratégies de contrôle de l'entreprise ; de s'impliquer dans l'amélioration des stratégies de contrôle et dans la réduction du niveau des risques ; de vérifier le contrôle des risques par l'organisation.

Toujours dans la pratique, quelles sont les responsabilités de l'auditeur interne ? Le cadre général est l'application du droit de la responsabilité civile en France. On rappelle tout d'abord que l'auditeur interne est un salarié. Il ne représente pas – comme par exemple un auditeur externe, un commissaire aux comptes – une profession réglementée. L'audit interne est une profession normée, mais non réglementée. L'auditeur interne n'est donc pas soumis à des obligations légales spécifiques susceptibles d'engager sa responsabilité. Il agit comme un salarié, conformément aux règles d'audit interne, mais il n'est pas infaillible.
Le rôle et les responsabilités de l'auditeur interne doivent être décrits dans la charte. Les chartes présentent l'intérêt de fixer les choses et de sensibiliser les différents acteurs qui travaillent sur le sujet de l'audit interne, des risques, du contrôle interne : la direction générale, le conseil d'administration ou le conseil de surveillance, des comités spécialisés rattachés au conseil d'administration… Il est bon de rappeler, dans une organisation, qui fait quoi, notamment en matière d'audit interne, de contrôle interne et de suivi des risques.

« Les auditeurs internes ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes. » La mise en œuvre de la responsabilité civile personnelle est exceptionnelle. Si un auditeur interne a failli, a mal rempli son rôle, s'il n'a pas assumé ses responsabilités, violé les normes professionnelles, il peut être licencié, en effet. Mais on ne lui demandera pas des dommages et intérêts sur ses deniers personnels. Il y aurait sanctions civiles avec versement de dommages et intérêts, pour un auditeur interne qui, par exemple, aurait divulgué des informations confidentielles ayant entraîné un préjudice. On applique alors les grands principes de responsabilité civile français : une faute, un dommage et un lien de causalité entre la faute commise et le dommage subi par une victime.
Il y a également des risques exceptionnels de mise en cause de responsabilité, si l'auditeur est actif dans la prévention et la détection des fraudes. La responsabilité pénale est envisageable en cas de complicité d'un auditeur interne dans un montage où il aura eu connaissance d'un dysfonctionnement qu'il aura volontairement caché. Etant complice d'une infraction, il peut être poursuivi, mais c'est vraiment exceptionnel.

L'ordonnance du 8 décembre 2008 a fait couler beaucoup d'encre. Cette ordonnance, rappelons-le, est une transposition de la 6e directive pour la création de comités d'audit dans certaines structures, notamment les sociétés cotées. Le comité d'audit est un comité spécialisé, rattaché à un conseil d'administration ou à un conseil de surveillance – ce n'est pas un comité opérationnel – et chargé du suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques. C'est un rôle nouveau pour le comité d'audit, donc pour le conseil d'administration puisque, rappelons-le, un comité d'audit ne prend pas de décision. Le comité d'audit aide le conseil d'administration ou de surveillance à prendre les décisions.

Quelle est l'incidence de l'ordonnance du 8 décembre 2008 sur la relation entre l'audit interne et le comité d'audit ? Les auditeurs internes et le comité d'audit travaillent régulièrement ensemble, ils sont complémentaires. Cela implique-t-il de nouvelles exigences vis-à-vis des auditeurs internes ?
La fonction d'audit, on le sait, doit être indépendante, disposer de moyens suffisants ; elle doit rendre compte au plus haut niveau de l'entreprise, donc au conseil d'administration et au comité d'audit. La répartition des rôles et responsabilités entre la direction générale, le conseil d'administration et le comité d'audit, en matière de suivi des risques, fait débat. Un groupe de travail, a été constitué par l'AMF, pour débattre sur le « suivi de l'efficacité » et les responsabilités des différents acteurs dans l'entreprise.

La question des recours éventuels en responsabilité se pose. Certains pensent que cela ne change rien pour les membres des comités d'audit. Ils agissent sous la responsabilité du conseil d'administration. L'ordonnance le précise. C'est donc le conseil d'administration qui sera responsable du suivi de l'efficacité. Cela étant, il n'existe pas en France de responsabilité collective. C'est une responsabilité individuelle. Mais on parle de responsabilité collective, parce que le conseil d'administration est un organe collégial, qui prend des décisions en votant, mais on peut aller chercher – rappelons l'affaire Rhodia, qui est en appel actuellement – la responsabilité d'un administrateur, voire de plusieurs, même pour des fautes différentes. On peut aller chercher leur responsabilité personnelle, sur le plan civil ; voire, dans des cas graves, sur le plan pénal.
Si je suis membre d'un comité d'audit, qui plus est, spécialisé en matière comptable ou financière, est-ce que je suis plus exposé ? Qu'est-ce que je vais demander aux auditeurs internes ? Est-ce que je vais davantage formaliser la relation entre le comité d'audit et les auditeurs internes ? On constate qu'au sein des conseils d'administration, on demande davantage de formalisation. Je m'explique : entre le conseil d'administration et le comité d'audit, les échanges étaient assez informels ; maintenant, une réflexion s'est instaurée sur la formalisation des travaux. Quand le conseil d'administration fait travailler le comité d'audit sur différents sujets, les échanges d'informations sont davantage formalisés. Quand un comité d'audit travaille sur un sujet, il interroge différents acteurs, dont des auditeurs internes, et les échanges sont formalisés. Les rapports devront être plus précis.

Je trouve que cette tendance accroît l'importance du rôle des auditeurs internes, qui sont de plus en plus sollicités par les conseils d'administration. Je pense qu'il y aura davantage d'échanges et de travail en commun entre le comité d'audit et les auditeurs internes, notamment sur le suivi des risques.

Il y a incontestablement une évolution. L'ordonnance de 2008 a modifié le rôle du comité d'audit et donc du conseil d'administration, et cela va sans doute changer les relations, et améliorer l'environnement de contrôle et le contrôle interne.

En conclusion, l'impératif est bien évidemment la souscription d'une police d'assurance adaptée, tant pour les administrateurs que pour les auditeurs internes.

Questions/Réponses

Question

Est-ce l'assurance la seule protection pour l'audit interne ? Est-ce que vous n'en voyez pas d'autre ?

Sylvie LE DAMANY

Si. C'était un peu caricatural. Il faut être assuré, comme un certain nombre de professions. Mais enfin, le plus sûr – vous le savez tous –, c'est d'avoir une fonction d'audit interne très forte, très bien organisée et qui travaille en étroite relation avec le comité d'audit.

Question

Concernant la 8e directive, vous avez dit : « Le comité d'audit doit assurer le suivi de l'efficacité. » Vous avez dit également : « Il est chargé de suivre l'efficacité ». Est-ce que c'est la même chose que « chargé d'assurer le suivi de l'efficacité » ?
L'ordonnance dit : « assurer le suivi », et dans le groupe de place on est très pointilleux sur chaque mot. Est-ce que pour vous, c'est la même chose ?

Sylvie LE DAMANY

Il faut en fait remonter à la directive et reprendre les termes anglais. Il y a tout un débat sur les terminologies. Je vous en ferai grâce, mais en effet, c'est : « suivre l'efficacité »

Question

Avez-vous une explication concernant la différence entre la directive et l'ordonnance ? Dans la directive, on parlait d'assurer le suivi de l'efficacité des systèmes de contrôle interne, d'audit interne le cas échéant et de gestion des risques. Or, dans l'ordonnance, l'aspect audit interne a été supprimé. Or, dans la quasi-totalité des transpositions dans les pays étrangers, celles-ci mettent en avant l'audit interne. Avez-vous une réponse sur ce point ?

Sylvie LE DAMANY

Non, je n'ai pas de réponse, mais il serait en effet intéressant de creuser ce point. Il y a parfois des oublis dans des textes rédigés un peu trop vite. Parfois c'est volontaire.

Question

Vous avez évoqué la responsabilité de l'audit interne, donc du contrôle périodique. Nous avons vu aujourd'hui que la lutte contre la fraude reposait aussi sur le contrôle permanent, avec des cellules de contrôle ad hoc, et des spécialistes de la lutte contre la fraude. Quid de la responsabilité de ce contrôle permanent ? Serait-elle totalement différente de celle de l'auditeur ? Est-ce que leur responsabilité est plus engagée, sachant qu'ils se consacrent spécifiquement à la fraude ?

Sylvie LE DAMANY

Ils ont en effet une spécialité, mais ils ne sont pas pour autant infaillibles. Ils sont exactement dans le même cas que les auditeurs.

Question

Ma question porte non pas sur la responsabilité civile mais sur la responsabilité pénale de l'auditeur. De ce que j'ai compris, vous avez indiqué que, globalement, celle-ci existe uniquement en cas de complicité, donc le problème est le même pour n'importe qui, qu'il soit auditeur ou non.
Mais on pourrait imaginer un cas dans lequel l'auditeur accomplit un certain nombre de diligences dans le cadre de ses fonctions, dans le cadre de la lettre de mission, pour détecter une éventuelle fraude. Et on peut imaginer une situation dans laquelle il va recouper des fichiers : fichiers fournisseurs, fichiers clients… et que, pour une raison quelconque, l'entreprise ne respecte pas les dispositions législatives et réglementaires en matière de fichiers.

Sylvie LE DAMANY

Les dispositions de la CNIL ?

Question

Oui, tout ce qui est relatif à la CNIL ou autre type d'infraction qu'il peut commettre, sans s'en rendre nécessairement compte, avec, pour conséquence, des éventuelles sanctions prises par l'entreprise à l'encontre du salarié, qui pourraient être déclarées irrecevables devant un conseil des prud'hommes.

Sylvie LE DAMANY

Perben II a permis de faire jouer la responsabilité pénale de la personne morale, avec un cumul possible avec des personnes physiques qui peuvent être des dirigeants, où des délégataires.
Pour pouvoir poursuivre le délégataire, il faudrait que l'on puisse prouver qu'il disposait des moyens, qu'on l'avait chargé de faire appliquer la loi dans ce domaine, et donc peser sur lui – mais en général, ce n'est pas l'auditeur interne, c'est le directeur des systèmes d'information ou le *compliance officer* qui a une délégation spécifique avec un transfert de responsabilité pénale. Là, je parle de la délégation au sens pénal, avec les pouvoirs qui lui sont conférés.
Dans ce cas-là, un salarié peut être impliqué, du fait de sa délégation au sens pénal, et à condition qu'il ait le pouvoir, les moyens… enfin que toutes les conditions jurisprudentielles soient réunies ; sa responsabilité pénale pourrait être engagée.

Question

Un certain nombre de cas ont été médiatisés, comme celui de la passerelle du bateau qui s'était effondrée, où des salariés sans délégation de pouvoir – et cela se voit de plus en plus souvent – sont poursuivis au pénal, pour des manquements à des obligations de prudence ou de sécurité. N'y a-t-il pas une jurisprudence qui commence à aller au-delà de la délégation de pouvoir, de la responsabilité pénale du simple dirigeant ou de la simple personne morale d'entreprise, et qui serait une responsabilité pénale du salarié.
Un auditeur qui ferait des recoupements de fichiers et des traitements non déclarés à la CNIL, commettant ainsi une infraction, pourquoi ne pourrait-il pas être poursuivi de la même manière ?

Sylvie LE DAMANY

Travaillant beaucoup sur ces sujets de responsabilité pénale dans les entreprises, je constate que les tribunaux sanctionnent la personne morale et les dirigeants, et des salariés délégataires, lorsqu'il n'y a vraiment pas de discussion sur la délégation au sens pénal. C'est plutôt bien cadré.

Frédéric GEOFFROY

Trois mots pour conclure.
J'ai été frappé de la convergence des préoccupations entre entreprises et intervenants qui travaillent dans des milieux très différents. J'ai été frappé aussi par le caractère évolutif du sujet, qu'il s'agisse des modèles d'organisation ou des aspects juridiques.
Je remercie tous les intervenants.