ifaci

institut français de l'audit et du contrôle internes

Actes du colloque

Comment devenir proactif dans la gestion de la fraude ?

Prévenir, détecter, traiter

mardi 23 novembre 2010

COMMENT DEVENIR PROACTIF DANS LA GESTION DE LA FRAUDE ?

PREVENIR, DETECTER, TRAITER

MARDI 23 NOVEMBRE 2010

Sommaire

INTRODUCTION, PAR ROMAIN MARIE 3

PRESENTATION DU CAHIER DE LA RECHERCHE, PAR JEAN-FRANÇOIS SAUTIN 4

ETHIQUE ET CRISES : QU'EST-CE QUE LES CRISES ONT CHANGE ? PAR MICHEL JORAS 6

AUDIT INTERNE ET FRAUDE : COMMENT L'AUDITEUR INTERNE PEUT-IL INTERVENIR A CHAQUE ETAPE DU DISPOSITIF ? PAR ERIC FREUDENREICH 10

L'INVESTIGATION INFORMATISEE DES FRAUDES : APPROCHES INFORMATIQUES ET CAS PRATIQUES 16
Pascal GADEA, *Directeur Commercial Grands Comptes France, ACL* 16
Noël PONS, *Consultant* 16
Yoanna PONS, *Auditeur S.I., Audéa* 16

COMMENT DEVENIR PROACTIF DANS LA PREVENTION ET LA DETECTION DE LA FRAUDE ? 24
Bernard DECOEUR, *Chargé de Mission, Direction Audit & Risques, Service du Contrôle Interne GDF SUEZ* 24
Emmanuel PASCAL, *Audit Manager, Brakes Group* 24
Hugh PENRI-WILLIAMS, *Administrateur, ACFE Chapitre France* 24

COMMENT UTILISER LA CARTOGRAPHIE DES RISQUES DANS LA PREVENTION ET L'ANTICIPATION DE LA FRAUDE, PAR SEBASTIEN ALLAIRE 31

LES ASPECTS JURIDIQUES LIES A LA FRAUDE, PAR JEAN-VICTOR PREVOST 35

COMMENT REAGIR FACE A UN SOUPÇON DE FRAUDE OU TRAITER D'UN CAS AVERE ? 39
Jean-François SAUTIN, *Président de l'Unité de Recherche, Senior vice-President Group Audit, Lafarge* 39
Emmanuel PASCAL, *Audit Manager, Brakes Group* 39

TABLE RONDE : QUELLE EST L'INCIDENCE DU SECTEUR D'ACTIVITE SUR LE DISPOSITIF DE LUTTE CONTRE LA FRAUDE ? 46
ANIME PAR ROMAIN MARIE, *Senior Vice-president Internal audit & Internal control, Alstom* 46
AVEC VALERIE BERCHE, DIRECTRICE AUDIT GROUPE, FRANÇAISE DES JEUX 46
MARC FOURRIER, DIRECTEUR DE LA CONFORMITE, ALLIANZ 46
MICHEL LAPORTE-MARROUX, INTERNATIONAL FRAUD & REVENUE ASSURANCE MANAGER, FRANCE TELECOM ORANGE 46
CATHERINE VAN DER LINDEN, DIRECTEUR SECTORIEL AUDIT GROUPE, COORDINATEUR RISQUES DE FRAUDE CORPORATE, TOTAL 46

INTRODUCTION, PAR ROMAIN MARIE

Louis VAURS

Je voudrais dire quelques mots sur l'importance du sujet. Le problème de la fraude intéresse toutes les organisations. On a vu les dégâts causés dans une grande entreprise bancaire touchée par une fraude majeure ; cela met en péril l'organisation elle-même, avec un sauvetage plus que difficile.

C'est une préoccupation des directions générales ; c'est également, par définition, une préoccupation des auditeurs internes ; et c'est également une préoccupation de l'IFACI : depuis maintenant plusieurs années, nous menons une réflexion permanente sur le sujet. Comme vous le savez peut-être, nous avons publié, il y a moins d'un an, un cahier de la recherche sur la fraude dans le secteur bancaire. Un nouveau cahier vous sera présenté tout à l'heure par le président du groupe de la recherche, Jean-François Sautin.

Romain MARIE, *Senior Vice-president Internal audit & Internal control, Alstom*

Je vous remercie de votre présence. Le sujet est d'intérêt, et nous avons un programme chargé.

Tout d'abord, M. Sautin va nous présenter le cahier de la recherche sur la fraude, en tant que président de l'unité de recherche.

Le thème suivant fera la liaison entre crises et éthique.

Nous enchaînerons sur un sujet propre à l'audit interne : comment l'auditeur interne peut-il intervenir à chaque étape du dispositif : prévenir, détecter, traiter ?

Nous poursuivrons avec l'investigation informatisée des fraudes : les approches informatiques et les cas pratiques.

Nous aurons une session sur le thème : comment devenir proactif dans la prévention et la détection de la fraude ? Nous sommes là au cœur du sujet.

Nous verrons comment utiliser la cartographie des risques dans la prévention et l'anticipation de la fraude.

Nous enchaînerons sur le sujet : comment réagir face à un soupçon de fraude ou traiter d'un cas avéré, sujet délicat s'il en est, et je parle d'expérience.

J'animerai une table ronde sur le sujet de l'incidence du secteur d'activité sur le dispositif de lutte contre la fraude.

Puis nous clôturerons cette journée.

PRESENTATION DU CAHIER DE LA RECHERCHE, PAR JEAN-FRANÇOIS SAUTIN

Jean-François SAUTIN, *président de l'unité de recherche, Senior vice President Group Audit, Lafarge*

Tous les chemins mènent à l'audit. Je suis ingénieur de formation. J'ai fait toute ma carrière chez Lafarge, pendant de nombreuses années, dans un domaine qui n'avait rien à voir avec le contrôle interne et l'audit ; je suis en charge de l'audit interne depuis quatre ans au sein de ce groupe international.

Je suis donc dans la position de quelqu'un qui a découvert la fonction, et qui a été confronté à la problématique de la fraude. Cela s'inscrit tout à fait dans le principe du cahier de la recherche. Mais avant de commencer ce cahier de la recherche, nous nous sommes interrogés : est-ce qu'on ne rajoutait pas une couche supplémentaire sur un terrain déjà très encombré ? Il existe une copieuse littérature sur le thème de la fraude, et de nombreuses références. Et, comme le soulignait Louis Vaurs il y a quelques minutes, en 2010, l'IFACI avait déjà publié un cahier de la recherche sur l'audit de la fraude dans le domaine bancaire et financier. Nous avons donc là un corpus de réflexion très riche.

Le thème de la fraude reste vraiment actuel. Noël Pons nous donne régulièrement des lectures intéressantes sur le sujet. Le public est très certainement intéressé par tous les cas de fraude récents qui ont touché les grands groupes. Les cabinets d'audit externe publient régulièrement des monographies sur la fraude, l'état de la fraude, l'impact de la fraude dans la crise, etc.

Nous nous sommes donc demandé où on allait se situer. Ce qui manquait peut-être, et là où l'on pouvait espérer avoir une valeur ajoutée pour les lecteurs potentiels de ce cahier de la recherche, c'était une **réflexion pédagogique** qui pourrait être utile à quelqu'un faisant partie d'un groupe d'audit interne ou de contrôle interne, confronté au thème de la fraude et qui chercherait à faire évoluer son organisation, pour une meilleure maîtrise de ce risque.

Comment entrer dans cette problématique ? Le groupe de recherche (rassemblant dix-huit professionnels) avait en fait un fil conducteur assez clair qui était de prendre la température d'une organisation, et d'évaluer le niveau de maturité de cette entité en matière de fraude. Quels conseils, quels cheminements proposer à des personnes qui vont être engagées dans la maîtrise du risque fraude, pour progresser ou faire progresser un dispositif qui existe, ou créer un dispositif qui n'existerait pas ? Or on s'aperçoit très vite qu'il n'y a pas de recette miracle : chaque cas est différent, chaque entreprise est différente. Comment adapter à l'activité propre ce dispositif ? Il fallait absolument faire quelque chose de pragmatique.

La fraude est un acte dissimulé, déplaisant. C'est quelque chose dont on n'a pas très envie de parler. Et souvent, dans les entreprises, on occulte un peu la question, ou l'on en parle dans un cercle très restreint. Notre Groupe de Recherche s'est en fait rendu compte très vite qu'il faut apprendre à en parler ; savoir le faire, c'est déjà commencer à résoudre le problème. Et il faut surtout s'arc-bouter sur la conviction que, de ce sujet déplaisant, on peut faire un moteur de motivation. Si la Direction est vraiment engagée dans un travail de fond sur la maîtrise du risque fraude, elle projette d'une part un sentiment de qualité, d'autre part un sentiment de justice (de par les sanctions prises), au moins aussi important.

Peut-être pourrait-on adopter une analogie médicale. En effet, la fraude est un peu comme une maladie de l'entreprise, et il y a, comme en médecine, plusieurs niveaux d'intervention. Il y a des niveaux d'hygiène et de prévention : tout ce qui est préparation, anticipation. Il y a des dépistages, et la cartographie des risques est un système de dépistage qui permet de mieux comprendre les épidémiologies. De temps en temps, il faut même avoir recours à la chirurgie.

Une conviction du groupe de travail est que la fraude n'est pas une affaire de spécialistes. Elle nécessite la mobilisation de l'ensemble des acteurs de l'organisation. Les personnes directement impliquées dans le contrôle interne ou dans l'audit interne ont un rôle plus fort d'animation, de développement, mais elles n'arriveront à rien si l'ensemble de l'organisation n'est pas mobilisé sur ce thème-là.

Au cours de nos travaux nous avons dû éviter deux pièges méthodologiques. Quand on parle de la fraude, on parle très souvent de psychologie ou de sociologie, de dimension éthique ; inversement, on peut aussi parler technicité, processus de contrôle interne. D'entrée de jeu, il nous a semblé important de ne pas réduire le cahier de la recherche à une dissertation éthique non plus qu'à un traité de contrôle interne, même s'il faut prendre en compte ces deux dimensions pour une meilleure maîtrise du risque de fraude.

Le cahier comporte six chapitres auxquels il sera fait allusion au cours de la journée. Un premier chapitre pose la question : de quoi parle-t-on ? Un certain nombre de définitions et de catégorisations existent déjà dans le monde du contrôle et de l'audit internes. Nous les avons utilisées.

Un deuxième chapitre traite des pré-requis pour atteindre à l'efficacité ? Il ne sert à rien de partir tout feu tout flamme à l'attaque du risque fraude si l'organisation n'est pas intéressée, si le ton de la direction générale n'est pas en ligne avec cet engagement, etc. Un certain nombre de points de repère apparaissent dans le cahier de la recherche, qui disent : lancez-vous dans l'action mais, auparavant, essayez de comprendre le contexte dans lequel votre organisation fonctionne.

Un troisième chapitre, très pragmatique, parle de la construction et du pilotage du dispositif. On revient là sur des sujets assez classiques que nous avons essayé de représenter, de restructurer, dans cette démarche pédagogique.

Un quatrième chapitre pose la question de savoir ce que l'on fait en cas de soupçon ou de cas avéré ? On entre alors dans un mode de gestion de crise. On y reviendra dans le courant de la journée.

Le cinquième chapitre traite de la cartographie du risque fraude ; il nous a paru important de porter un éclairage spécifique sur cet outil de base.

Le sixième chapitre présente une série de fiches pratiques. Je vous disais en introduction que l'on a essayé d'être le plus pragmatique possible.

Je vais passer d'une analogie médicale à une analogie culinaire. J'espère que ce cahier est plus qu'un livre de recettes, qu'il est une introduction à la haute cuisine, avec, si possible, de temps en temps, quelques recettes qu'il appartiendra aux lecteurs d'adapter, de transformer en fonction du contexte spécifique de chaque entreprise et de chaque équipe.

Dix-huit professionnels de talent ont travaillé dans ce groupe de travail et je voudrais ici les remercier. Ce cahier représente à peu près une année de travail, beaucoup de réunions, d'échanges, de rédaction en groupe, ce qui est toujours un exercice périlleux.

ETHIQUE ET CRISES : QU'EST-CE QUE LES CRISES ONT CHANGE ? PAR MICHEL JORAS

Michel JORAS, *Enseignant Chercheur, HDR ESCE Paris*

Il est un peu utopique, en vingt minutes, de parler du changement du monde qui, à mon avis, depuis la chute du mur de Berlin, en 1991, a totalement bouleversé notre quiétude , axée sur le consensus de Washington où tout était régulé par le marché seul Nous nous trouvons maintenant devant cette crise systémique depuis 2008, qui remet totalement « les pendules à l'heure de la nouvelle réalité. » La dernière crise monétaire de l'Irlande appelle évidemment notre attention.

Je voudrais simplement, en quelques instants, vous parler des crises éthiques que nous subissons depuis 1991 et, réussir à vous expliquer que ces crises éthiques, comme toutes les crises, mettent le monde face aux défaillances de certains processus de la gouvernance des risques financiers et bancaires Une crise éthique est une situation hors contrôle éthique des acteurs , suite à des comportements inéthiques, dangereux , menaçants, dommageables pour la conformité et la sureté éthiques ; c'est un affaissement brusque des soutiens que sont les règles et les principes éthiques dans un système de décision, de management, de gouvernance.

Ces crises métamorphosent le monde économique. Ce nouveau monde cherche à remettre en évidence un fort besoin d'éthique. On a vu ce mot apparaître dans la conduite des affaires il y a une trentaine d'années, on ne savait pas bien ce que c'était, était-ce de la morale, de la conscience ? Aujourd'hui, cent pays se sont mis d'accord, avec ISO International, pour enfin donner à l'éthique une définition laïque basée sur des comportements éthiques désignés et en accord avec les attentes de la communauté des hommes (iso 26000)

Quelles sont les suites de ces crises éthiques ? Vous savez que les crises produisent en général de la haine, des peurs. On recherche des coupables. Et on redemande de la régulation, de la vigilance ; l'obligation de vigilance et l'obligation de précaution interpellent le management. Et , enfin, on s'efforce alors d'établir un code universel pour fixer ce que l'on appelle les règles du jeu, moins laxistes C'est la grande évolution qui est en train de se mettre en place et de s'imposer dans le management international

Je voudrais vous expliquer que ces crises, on les subit durement. Il y a d'abord eu Tchernobyl. C'était la fin de l'arrogance technologique. Après, il y a eu Enron, et l'on a vu que les commissaires aux comptes n'étaient pas toujours très éthiques. Puis ce fut la crise systémique des *subprimes*. Et tout récemment, la crise monétaire de pays de l'EURO, la Grèce et l'Irlande.

Ces crises entraînent des obligations plus strictes de contrôle, de vigilance et donc d'éthique. Cette éthique nouvelle vient mettre un terme à trente ans de combats épistémiques, éthique des affaires, éthique des organisations ?; est-ce l'éthique anglaise, américaine qui est de la conformité, mais surtout de la promesse de tenir ses engagements (soft law)? Est-ce l'éthique à la française, le seul respect des règles du droit (hard law).Le monde de la normalisation, ISO, vient de se mettre d' accord sur une éthique normée qui, au fond, ne devient » qu'un comportement, c'est-à-dire une conduite juste et bonne, dans une situation donnée et en cohérence avec les normes internationales. » (iso 26000).

De fait, il n'y a pas une éthique, il y a des éthiques. En réalité, la base de l'éthique dans notre monde occidental, c'est : ne pas nuire à autrui. Est-ce pourquoi voit-on arriver cette idée que les sciences de l'ingénieur, les sciences des gestionnaires rejoignent les sciences du vivant et côtoient l'éthique médicale et de la santé.

Cette grande évolution qui vient de se produire, après dix ans de travail, à ISO International, c'est se rendre compte que l'éthique c'est aussi respecter les attentes des droits coutumiers et des droits internationaux universellement reconnus ou quasi reconnus (iso 26000).

L'éthique doit donc être retenue et vécue dans une situation donnée, acceptée et reconnue par les autres. Ce qui fait que cette éthique nouvelle devient une discipline à part entière. Comme il y a eu la naissance des sciences de gestion après 1968, se met en place ce que j'appelle une éthique managériale dont l'enseignement intègre déjà les grandes écoles et les universités. Comme il y a eu le contrôle de gestion, comme il y a eu l'audit social, on voit apparaître cette nouvelle discipline qu'est l'éthique managériale.

La conformité éthique est un contrôle constant du respect, par les acteurs de la sphère d'influence, du cadre réglementaire et des engagements selon les principes reconnus. Pour nous, les Français, qui sommes germano-latins, l'éthique, c'est respecter le droit seul. L'évolution actuelle, est que nous rentrons dans un monde un peu plus religieux, typiquement anglo-américain où être éthique, c'est respecter la promesse et ou l'on voit apparaître trois obligations morales fortes, faire preuve de transparence , éviter le mensonge, proscrire les conflits d'intérêt.

La sûreté éthique est un état de contrôle raisonnable du maintien de cette conformité éthique et c'est un devoir de vigilance. Ce devoir de vigilance qui n'était pas normalement de l'obligation du directeur des ressources humaines (ou du directeur de l'entreprise) , fait que celui-ci, doit non seulement maximiser ses ressources humaines, bien les choisir, les protéger, bien les payer, bien les traiter mais encore s'en protéger , c'est-à-dire vérifier que ces mêmes ressources humaines ne sont pas des menaces de risques potentiels C'est une révolution mentale qui bouleverse évidemment la posture de la gestion des ressources humaines classique.

Et vous, membres de l'IFACI dans le domaine du contrôle, non seulement vous devrez contrôler les faits, les chiffres, mais vous allez également avoir à contrôler quelque chose de beaucoup plus subtil, très subjectif, ce que l'on appelle les comportements humains et leurs dérives éventuelles

Après cette première refondation que je vais appeler conceptuelle et même mentale, nous en arrivons à l'institutionnalisation de cette sureté éthique et son management, que nous dénommons dorénavant éthique managériale ou des managers, collectivement ou individuellement concernés Lorsqu'une nouvelle discipline se met en place dans le monde du management , elle le fait avec des supports nouveaux, c'est-à-dire des colloques, des conférences, des conventions, La communauté européenne , émet alors des directives. Et la France, bien entendu, est obligée d'adapter le droit européen en créant des institutions et des professions correspondantes

Notre société s'oblige ainsi à renverser totalement son regard sur le monde. Jusqu'à maintenant, on se préoccupait de la morale des individus, dorénavant de la déontologie des professions, de la responsabilité sociétale de l'entreprise. Nous avons renversé le « sablier », nous sommes amenés à réformer la gestion des entreprises, non plus par des seules règles de droit mais par des dispositifs, mais par des principes, lignes directrices basées sur des attentes de la communauté humaine.

En France, cette institutionnalisation se fait évidemment sous la supervision des services centraux et par la création de tout un ensemble d'organismes : par exemple, la HALDE, la Commission Informatique et Libertés, les services d'inspection des ministères, des agences de la Santé, de la Sécurité informatique, le comité d'éthique médicale, les douanes, etc.

En réalité, on voit que l'Etat régulateur se préoccupe beaucoup plus d'être un Etat du contrôle de moralisation qu'un contrôle de décision. ? C'est une transformation difficile à comprendre : l'Etat ne va pas être celui qui décide mais celui qui va essayer de proposer, réguler, de médiatiser, d'assister.et naturellement de réprimer si les intérêts nationaux sont affectés

Ce changement de paradigme de la gouvernance est assez déroutant puisque que l'on est passé, en même temps , d'un monde d'énarques, de hauts fonctionnaires à un monde d'avocats, qui n'ont pas, du tout , les mêmes dispositions à l égard du gouvernement de l'Etat et de sa gouvernance.

Cette sûreté éthique et sa maitrise amènent tous les dirigeants non seulement à protéger les acteurs économiques et sociaux mais à s'en protéger. C'est pourquoi se mettent en place des institutions, des règles et une nouvelle discipline autour du contrôle, qui a tendance à vouloir rapprocher sinon fusionner des métiers, jusqu'alors différents : l'inspection, le contrôle, l'audit, l'éthique managériale, la gestion des risques, la répression des fraudes, etc.

Cette fusion va provoquer un bouleversement stressant dans tout ce qui est le contrôle, puisque nous allons assister à l'arrivée d'un nouveau type d'individu que l'on connaît mal. Avant, il y avait le commissaire aux comptes, les correspondants informatiques et liberté, des responsables de la conformité et du contrôle interne, les inspecteurs du travail. , les responsables des douanes, les inspecteurs des grands corps de l'Etat, les médiateurs, etc., demain des Responsables indépendants des conformités éthiques agissant sous des appellations diverses

Et on voit bien que ce changement est de vouloir et pouvoir croiser, métisser les activités des associations aux domaines proches mais indépendants : à titre d'exemples, l'IFACI, du contrôle interne, l'AFAI des auditeurs et conseils en informatique , l'IAS , dont je suis un des fondateurs, qui s'occupe de l'audit social ; PROMETHICS, une association qui certifie les auditeurs éthiciens, etc.

Vous connaissez la roue de Deming : *plan*, *do*, *check, act*. Eh bien, ce changement des repères amène à mélanger la fonction *check* et la fonction *act*. On constate dans les banques une confusion entre les métiers de l'inspection, les métiers de l'audit, les métiers du contrôle des risques, les déontologues.

Ces métiers de la conformité chez nos amis anglo-saxons, s'appellent *Compliance Officer*s Or en réalité, on ne sait pas bien définir ce qu'est la *compliance*. La *compliance*, c'est non seulement la conformité aux règles, non seulement la conformité aux promesses, non seulement la conformité aux attentes, mais c'est aussi une mission permanente du contrôle des risques .Moi qui, depuis 1950, a vu le changement permanent de nos sociétés, je pense que nous assistons au changement des disciplines, des diligences et méthodes de contrôle, et que les métiers du contrôle, de l'audit, de l'inspection, de la médiation, ce que l'on appelle aussi des *coachs*, des supports, et je suppose que tout cet ensemble va très certainement occuper au moins le tiers de toutes les activités humaines. Pour conclure, je voudrais faire passer un peu de peur dans l'assistance. Car en réalité, si l'on devient plus éthique, c'est uniquement parce que l'on a peur. Et je vois apparaître la plus grande menace, contreface du progrès du web, la cybercriminalité et les catastrophes inconnues provoquées Et, vous qui vous consacrez au contrôle, vous allez non seulement avoir à contrôler les entreprises, leurs fonctions, leurs résultats, mais vous allez aussi avoir à contrôler cette matière virtuelle que l'on appelle les réseaux sociaux, les réseaux humains. Non seulement le contrôle va être obligé de s'occuper d'entités avec des structures reconnues, avec des frontières, avec des espaces bien compris, mais également des entités avec des espaces inconnus, un peu comme celle des neurones du cerveau humain. Ce qui fait que vous allez être obligés constamment de penser que le contrôle classique n'est plus suffisant.

La fonction majeure dans le monde moderne sera le contrôle du contrôle pour éviter les crises éthiques Et je pense personnellement que les commissaires aux comptes deviendront des commissaires à l'éthique ou des commissaires au contrôle du contrôle.

Construire l'avenir conduit au-delà du doute et de l'utopie

Merci de votre attention.

QUESTIONS/REPONSES

Louis VAURS

Merci pour votre très brillante intervention. Vous avez mis en avant un certain nombre de points sur lesquels j'aimerais revenir, si vous le permettez.

Je crois que vous avez bien vu que, dans le monde actuel, il existe toute une série de fonctions qui gravitent autour du contrôle interne, et cela peut éventuellement poser des problèmes. C'est une de nos préoccupations. Il est indispensable qu'il y ait une coordination entre l'ensemble des fonctions que vous avez énumérées tout à l'heure. Et s'il n'y a pas cette coordination, il y a deux risques : le trou dans la raquette, c'est-à-dire que l'on ne voit pas ce qui se passe ; ou bien une redondance.

Je voudrais apporter une précision concernant le secteur bancaire. Vous avez énuméré l'inspection, l'audit, la conformité, le contrôle interne. Mais là, il n'y a pas de confusion, bien au contraire, puisqu'il y a une séparation stricte entre l'ensemble de ces fonctions, chacune d'elles ayant, en principe, un rôle bien défini.

Michel JORAS

Je crois que je me suis mal exprimé. Je pense qu'il y a deux fonctions séparées, deux métiers différents mais proches: le contrôle interne et le contrôle externe. Et il y aura un autre contrôle qui sera le contrôle de ceux qui contrôlent, c'est-à-dire que l'on va vers un monde de certification. Ce contrôle va donc avoir trois pieds : le contrôle interne, ce que j'appelle la conformité interne ; la conformité externe ; et un troisième la conformité de la conformité interne et de la conformité externe.

Louis VAURS

A l'IFACI, on a l'habitude de mettre en avant trois lignes de défense : une première ligne qui est constitué d'opérationnels ; une deuxième ligne qui comprend, entre autres, le contrôle interne et la gestion des risques ; la troisième ligne, c'est l'audit interne. Il existe enfin une quatrième ligne de défense, les auditeurs externes.

J'ai une question : quelle différence faites-vous entre éthique et déontologie ?

Michel JORAS,

C'est très simple : l'éthique est une façon de faire, c'est un comportement des individus, des entreprises et des collectivités. Ce sont des bonnes pratiques et, des bonnes et justes conduites. Alors que la déontologie, ce sont des obligations de devoirs et des droits d'une profession. L'éthique, c'est donc le niveau supérieur, celui du management.

AUDIT INTERNE ET FRAUDE : COMMENT L'AUDITEUR INTERNE PEUT-IL INTERVENIR A CHAQUE ETAPE DU DISPOSITIF ? PAR ERIC FREUDENREICH

Eric FREUDENREICH*, Contrôleur financier de la division Energie & Industrie, Vallourec*

Je suis contrôleur financier, ce qui fait que je joue entre la première et la deuxième ligne de défense, pour éviter toute confusion. En tant que joueur dans la première et la seconde défense, et fort d'une certaine expertise et de l'enseignement, mon objectif est aujourd'hui de partager avec vous ce que j'ai pu comprendre des normes. Il est peut-être plus facile pour moi de parler des normes que lorsque l'on en est vraiment responsable.

Pourquoi est-ce important ? M. JORAS a voulu vous faire peur. J'aurais préféré éviter d'en faire autant, mais l'actualité fait effectivement peur.

Je prendrai dans l'actualité les sanctions de l'AMF, qui datent de décembre 2009, à l'encontre d'une société que je ne nommerai pas. Il s'agissait de sanctions pécuniaires à l'encontre du dirigeant, ce qui est compréhensible, et à l'encontre d'un salarié, ce qui est un peu plus surprenant, car il n'était pas mandataire social ; la sanction n'est pas passée très loin des commissaires aux comptes. Qu'est-ce qui les a sauvés ? C'est la NEP 320. Ce n'est pas le sujet d'aujourd'hui, mais la NEP 320 est une norme d'exercice professionnel.

Je fais là un grand écart entre les sanctions envers le salarié, je me projette un peu dans le futur et je me demande : si demain, un directeur de l'audit interne est entendu, quel est le moyen pour lui, quelle est la parade pour ne pas être sanctionné ? C'est peut-être la même que celle utilisée par les commissaires aux comptes, c'est-à-dire les normes.

Les normes, ce n'est pas quelque chose de statique, c'est quelque chose qui évolue, qui évolue dans le temps, qui donne lieu à interprétation ; et elles ne sont pas toujours évidentes à interpréter. Les normes sont très vastes. L'objectif est de partager avec vous certaines recherches personnelles, dans le cadre de l'enseignement universitaire, sur ces normes, de les faire parler.

L'interprétation de l'IFACI nous est fort utile, mais il faut aller très loin dans la recherche pour se faire sa propre idée et valider cette propre idée. Le sujet qui m'amène, le rôle de l'auditeur interne dans les différentes étapes, je vais vous le présenter en deux volets principaux. D'abord les normes, que l'on va essayer de faire parler. Et l'implication de l'auditeur interne dans les différentes étapes pour prévenir, détecter ou traiter la fraude.

La pratique est incontestable, c'est-à-dire que le responsable d'audit interne est amené à jouer un rôle dans la phase d'investigation. L'enquête de l'IFACI, effectuée en 2009, révèle que 63 % des répondants ont pratiqué l'investigation. 72 % ne l'ont pas pratiqué mais en ont la responsabilité. Selon le CBOK, les compétences de l'auditeur interne, en matière de fraude prêtent parfois à discussion. Les compétences juridiques et la sensibilité à la fraude – en anglais, *awareness* – sont considérées comme plus importantes pour les responsables d'audit interne, et pas si vitales pour les auditeurs, superviseurs et managers. On va voir ce qu'il en est vraiment.

Il existe des différences entre l'audit interne et l'expertise (*Fraud Examiner)*. Par exemple, un des objectifs pour l'audit est de formuler une opinion. Pour l'expertise, c'est d'imputer une faute, ou de disculper une personne qui peut être soupçonnée de fraude à tort.

La fraude est explicite dans le cadre normatif international (CRIPP). Il existe des dispositions obligatoires ; obligatoires pour ceux qui ont compris l'intérêt d'utiliser les normes d'audit, pas obligatoires au sens légal. Ce sont les *Mandatory Recommendations*. Et il existe des dispositions *strongly recommended*, fortement recommandées. C'est une manière de dire que certaines normes prévalent sur d'autres.

Le terme « fraude » apparaît, en 2009, dans un certain nombre de normes sur la compétence, la conscience professionnelle, le *reporting*, le management des risques et les objectifs de la mission. Les dispositions sont renforcées. Suivre l'évolution des normes permet de mieux les comprendre, de les regarder sous un autre angle.

Les normes s'imbriquent dans un cadre de compétences. Du responsable de l'audit interne (RAI) on attend un degré de maîtrise de niveau 4 sur une échelle de 4 ; pour le senior, un niveau 3 ; et pour le junior, un niveau de 1 à 2. Le premier niveau, c'est d'avoir conscience de la problématique. Le deuxième niveau, c'est d'avoir une compétence *collective*. Le troisième niveau suppose un degré de maîtrise dans des situations simples, de façon autonome, indépendante. Le quatrième niveau, requis pour le RAI – et c'est une grande responsabilité – est d'être autonome dans des situations complexes.

Nous allons passer en revue les particularités de ces normes, d'abord de **qualification**, ensuite de **fonctionnement**.

La première norme de qualification, touchant à la **compétence** (norme 1210), dit que l'audit interne évalue le risque de fraude et la façon dont ce risque est géré par l'organisation. En anglais, il s'agit de *proficiency*, la capacité. Il faut être capable de…, ce n'est pas simplement d'être désigné *Certified Internal Auditor*, il faut en avoir les capacités. Et on voit que ces capacités peuvent être collectives – il ne faut pas tout porter sur ses épaules – et on verra que l'on peut aussi faire appel à des consultants ou à des ressources externes.

L'audit interne n'est pas censé posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes. Sur cette particularité, il ne faut surtout pas prendre de raccourci. La norme précédente demandait aux responsables d'audit interne, aux auditeurs internes d'avoir une connaissance suffisante des indices de fraude. Le raccourci serait de dire : la norme ne l'exige plus. Mais je pense que reconnaître les indices de fraude, c'est le minimum que l'on peut attendre de la part d'un responsable d'audit interne. On ne lui demande pas de la traiter mais de reconnaître les symptômes. Pour être plus précis, ce n'est pas un symptôme de fraude qui nous intéresse, c'est la combinaison de plusieurs symptômes. Les symptômes sont multiples, sont de différentes natures, et c'est cette combinaison qui devrait alerter l'auditeur interne.

La norme de qualification 1220 concerne l'étendue des **missions d'assurance**. On a ajouté le terme de « fraude » au terme « d'irrégularité ». L'irrégularité est quelque chose qui est contraire aux règles et la fraude est tout simplement l'addition des irrégularités et des actes illégaux. On traitait donc les irrégularités, et indirectement la fraude, sans la nommer.

La norme de fonctionnement 2060 traite du *reporting* à la direction générale et au conseil. Le risque de fraude doit faire l'objet du *reporting*. Cette norme avait déjà évolué en 2004. Avant 2004, on demandait un *reporting* avec une périodicité annuelle ou plus fréquente, si nécessaire. A compter de 2004, on a demandé un *reporting* pluriannuel. La norme demande les problématiques d'exposition aux risques significatifs.

La norme 2120 requiert d'évaluer le risque de fraude. Il s'agit d'évaluer l'environnement de contrôle, la gestion de la problématique d'éthique, et la culture éthique de l'entreprise guidée par l'exemplarité. Cette norme, et ses interprétations, mettent en garde contre les occurrences faibles ; une occurrence faible pouvant avoir un impact, un préjudice important. Cette norme dit également que, si la matérialité est difficile à chiffrer, il faut quand même essayer de la chiffrer. La dernière précision sur cette norme est que la prise en compte de la fraude au cours de la mission doit prévaloir sur l'audit spécifique de fraude. On va voir ce qu'est exactement un audit spécifique de fraude. Et le fait d'en avoir conscience tout au long de sa mission et de se poser des questions sur les symptômes de fraude vaut largement autant que de diligenter symboliquement des missions pour détecter des fraudes ayant ce seul objet.

La norme 2210, a trait à la probabilité d'erreurs significatives. Le terme « significatives » a été rajouté. L'IIA et l'IFACI jouent bien leur rôle pour défendre la profession : ce terme-là n'est pas anodin, en ce qui concerne la responsabilité. Et toujours le terme « fraude » est venu élargir le champ qui était limité aux irrégularités.

Sur les **interventions de l'audit interne**, nous allons porter un regard croisé sur les experts en fraude, les *Fraud Examiners* – ici experts légistes, pour éviter toute confusion ; sur la vision de l'IIA et sur notre propre vision.

Les experts légistes ont un rôle d'assistance dans la prévention et la détection de la fraude. Le management, ou d'autres autorités compétentes, dans les différentes lignes de défense, sont responsables de la prévention. Toutefois, l'expert en fraude est supposé suivre activement et recommander les procédures et les politiques de prévention de la fraude. Mais c'est le management et les autres autorités, les nouvelles fonctions créées et décrites par Michel Joras qui vont être responsables de la prévention, donc en amont de la détection.

La détection – et là, c'est un peu choquant – de la fraude est de la responsabilité première des auditeurs internes et externes. C'est la vision de l'ACFE. Elle peut être discutée, mais il est important de savoir comment nous sommes regardés par les autres autorités compétentes dans une entreprise, en ce qui concerne la fraude.

Le *Fraud Examiner Manual* mentionne spécifiquement les auditeurs internes pour : revoir les preuves écrites internes ; évaluer les indications ou plaintes (« Evaluer les indications » est une traduction… C'est la délation qui est derrière, c'est le cas où l'auditeur interne pourrait presque être amené à gérer l'alerte éthique, ou en tout cas à évaluer les alertes éthiques, ce qui est difficilement concevable) ; établir la liste des pertes et fournir une assistance dans les domaines techniques des activités de l'entreprise.

Selon l'IIA, le rôle de l'audit interne dépend du rôle qui lui est dévolu dans la charte d'audit interne et dans les politiques fraudes, ainsi que des services de conseils et de spécialistes attendus par le management et le conseil. L'IIA est très cohérente, elle renvoie à son cadre, à la définition de l'audit interne.

Et l'on rappelle quelque part que l'audit interne est une fonction qui apporte de la valeur ajoutée, qui peut être de l'assurance mais qui peut être aussi du conseil.

Les étapes du dispositif sont au nombre de cinq : **évaluer le risque** ; **prévenir et détecter** ; **mener des investigations** ; **auditer la fraude**.

Pour **évaluer le risque**, on dispose d'un éventail de missions que l'auditeur interne peut être amené à réaliser. Cet éventail est composé de trois volets. Le premier représente le rôle principal de l'audit interne : ce sont toutes missions d'assurance et d'évaluation. Le deuxième volet met en avant le rôle de conseil de l'audit interne vis-à-vis de la direction générale et du management. Le troisième volet indique les rôles que l'audit interne ne devrait pas endosser : responsabilité de la gestion des risques par exemple.

La **prévention**. Le principal mécanisme de prévention est le contrôle interne. La valeur ajoutée de l'audit interne est d'évaluer l'adéquation et l'efficacité du système de contrôle interne de l'organisation et l'exposition potentielle à l'organisation de la fraude.

La **détection**. Les responsabilités qui incombent à l'auditeur interne, en matière de détection de la fraude, sont au nombre de cinq : tenir compte des risques de fraude pour évaluer la pertinence des contrôles et déterminer les travaux d'audit à réaliser ; posséder une connaissance suffisante de fraude pour pouvoir déceler les indices (*red flags*) d'une fraude éventuelle, un indice pouvant être par exemple une exception aux procédures financières habituelles : paiement par chèque au lieu d'un virement ; faire preuve de vigilance dans les situations propices à la fraude, notamment en cas de contrôles déficients : tout contrôle déficient est une opportunité pour le fraudeur ; évaluer les

indices de fraude et décider si d'autres mesures sont nécessaires ou si une enquête doit être recommandée ; informer les autorités compétences au sein de l'organisation s'il s'avère qu'une fraude a été commise, afin qu'une enquête soit recommandée.

L'investigation. Dans cette phase, les parties prenantes sont les auditeurs internes, le responsable juridique, des enquêteurs et des experts légistes, le personnel de sécurité, d'autres employés non auditeurs. Dans le traitement de la fraude, l'aspect collectif est très important. Si le rapport d'audit interne ou le rapport d'expertise en fraude qui sera remis à l'issue de l'investigation n'est pas compréhensible pour le directeur juridique, j'ai des doutes sur le fait qu'il puisse ensuite être compris par un juge ou un avocat. Il faut donc faire revoir sa copie par d'autres corps de métier. On ne peut pas traiter la fraude tout seul, sans faire appel à d'autres intervenants. Une combinaison de compétences internes et externes est souvent nécessaire.

L'**audit de fraude**. Il peut exister une confusion entre investigation et audit de fraude. L'audit de fraude est une intervention post investigation pour éviter que la fraude se renouvelle par exemple. Lorsqu'une fraude est survenue, l'audit interne devrait concevoir des étapes supplémentaires dans le programme d'audit routinier ou développer des programmes d' « audit de fraude » qui aideront à révéler l'existence de fraudes similaires dans le futur. L'investigation n'est donc pas l'audit de fraude. L'audit de fraude est un exercice bien spécifique et qu'on utilisera de façon démarquée.

Il faut donc retenir que les dispositions ont été renforcées en 2009, avec des responsabilités accrues pour l'audit interne. Celui-ci doit posséder une connaissance suffisante pour pouvoir déceler les indices de fraude et recommander une investigation appropriée, si les circonstances le justifient. Selon la *Treadway Commission*, l'audit interne ne doit pas seulement avoir le soutien de la direction générale, mais aussi les nécessaires ressources pour exercer sa mission.

Finalement, tout est une question de compétence. Une implication plus importante dans l'éventail des missions nécessite donc un degré de compétence plus élevé et je pense que, lorsque l'on ne dispose pas des ressources avec ces compétences plus élevées, le garde-fou est d'éviter de donner une assurance à la direction générale.

En matière d'investigation, l'auditeur interne peut en avoir la responsabilité première, ou agir en tant que ressource, ou s'abstenir d'intervenir lui-même, parce qu'il est responsable de l'évaluation de l'efficacité des investigations.

L'audit interne peut exprimer une opinion sur le contrôle interne lié à la fraude. Dans les organisations la responsabilité première, en matière d'investigation, n'incombe pas à l'audit interne, mais les auditeurs peuvent tout de même être sollicités pour aider à collecter des informations et effectuer des recommandations pour l'amélioration du contrôle interne. En conclusion, toute intervention est acceptable si l'impact des activités sur l'**indépendance** des auditeurs internes est reconnu et pris en compte de façon appropriée ; et si les équipes d'investigation possèdent suffisamment de **connaissance** des schémas de fraude, des techniques d'investigations et des législations locales.

Je vais conclure en poursuivant l'analogie médicale de Jean-François Sautin. C'est une analogie avec le chirurgien-dentiste, métier que je ne maîtrise pas du tout. Il y a 35 ans, l'OMS a noté qu'après 30 ou 40 ans, on perdait davantage ses dents, non pas à cause des caries mais à cause de la parodontite. A la fin des années 1990, les dentistes, pour sensibiliser leur corps de métier, ont inventé un terme qui est la parodonto-conscience. Votre dentiste est parodonto-conscient ou il n'est pas parodonto-conscient. Lors d'un colloque, en l'an 2000, un chirurgien a dit : « Dès lors qu'un dentiste est parodonto-conscient et averti, il peut traiter 80 % des problèmes de ses patients en matière de parodontite. »

Pour l'auditeur interne, il faudra inventer un terme, car je pense qu'il est aussi un omnipraticien, comme le dentiste. Il sera donc tout à fait capable de traiter 80 % des problématiques de fraude de l'entreprise. Et les 20 % restant seront pour les spécialistes de la matière.

Comment devenir proactif dans la gestion de la fraude ?

QUESTIONS/REPONSES

Question de la salle

Votre présentation me laisse un peu confuse et soulève pas mal de questions. Dans nos missions d'audit aujourd'hui, on indique qu'il faut évaluer le risque de fraude potentiel.

A travers ce que vous avez démontré, j'ai l'impression qu'il ne vaudrait mieux pas.

Ai-je mal compris ? Est-ce qu'on prend un risque, en faisant cela ?

Eric FREUDENREICH

Si vous n'évaluez pas le risque de fraude, vous ne respectez pas les normes. Souvent, dans les cas de fraude, une des mesures correctives est d'avoir un audit interne efficace ou structuré. Qu'est-ce qu'un audit interne structuré ? C'est celui qui tend à se rapprocher de l'excellence. Et pour se rapprocher de l'excellence, il faut quand même respecter quelques normes, si on n'y arrive pas pour toutes.

La politique de l'autruche n'améliore donc pas, je pense, la situation. Sinon, il n'y aura pas seulement une déficience de contrôle interne ou d'évaluation du risque de fraude, mais une déficience d'organisation de l'audit interne.

Cela dit, je comprends que vous puissiez être confuse quand on vous présente ceci sous l'angle de la responsabilité.

Mais il ne faut pas adopter la technique des trois singes : je n'ai rien vu, je n'ai rien entendu, je n'ai rien dit ». Dans le droit français, cela peut effectivement encore fonctionner quelque temps, mais dans le droit international, le fait de ne pas faire, de ne pas voir et de ne pas entendre ne dégage pas la responsabilité.

En tout cas, au-delà de la responsabilité juridique, je pense qu'il y a aussi la conscience professionnelle. La conscience professionnelle, en anglais – et c'est très bien traduit dans la norme complète –, c'est *due professional care*. C'est le soin, le professionnalisme qui est attendu de vous, que vous apportez à l'entreprise. Cela va donc au-delà de la simple bonne conscience.

Question de la salle

J'ai une question concernant le chiffrage, en termes de détection, prévention. Savez-vous s'il existe un référentiel ? Sinon, quelles sont les bonnes pratiques par rapport à ce chiffrage ? Par exemple, le pourcentage du chiffre d'affaires pourrait-il être un indicateur ?

Eric FREUDENREICH

Je parle des normes en général, et pas seulement des normes d'audit interne et d'audit externe. Le chiffrage est toujours un problème. Il n'y a pas de normes, il y a des bonnes pratiques.

On prend effectivement les indicateurs financiers clés et on applique un pourcentage. On essaie de voir un impact. Ensuite, l'impact n'est pas que financier, cela peut aussi être indirectement un impact d'image, qui peut aussi indirectement coûter cher.

Beaucoup d'entre nous, dans leur parcours, ont fait un passage dans le commissariat aux comptes. Je pense que les seuils fixés par les cabinets, mais pas par leurs normes, sont utiles. Cela peut donner une idée. Finalement, le risque de fraude n'est qu'un risque parmi d'autres. Il ne faut pas non plus noircir le tableau, c'est un risque comme beaucoup d'autres dans l'entreprise.

Il faut aussi éviter de couper les cheveux en quatre et de vouloir chiffrer à tout prix, sur des tableaux très denses, l'impact d'une fraude. Je pense qu'il faut en permanence, un peu comme dans la roue de Deming mentionnée par Michel JORAS, revenir au point de départ et raisonner en grandes masses, raisonner en grands risques : quels sont les risques de mon secteur ? Je suis dans la téléphonie, je suis dans le pétrole, ce ne sont pas les mêmes risques de fraude.

Si on s'attelle déjà aux grands risques que toute personne expérimentée dans le métier connaît sur le bout des doigts, c'est alors un partage de savoir avec ces personnes, c'est une réflexion sur l'historique de l'entreprise qui permettent d'éviter de se noyer dans un tableau d'analyses méticuleuses.

Question de la salle

J'ai un commentaire. Au tout début, si j'ai bien compris, vous évoquiez le fait que, lors d'un rapport d'investigation, l'expert doit imputer la faute. Là-dessus, j'ai une réserve : pour moi, imputer la faute, c'est le rôle des autorités judiciaires compétentes, mais pas de l'auditeur interne, ni de l'expert, ni du *Fraud Examiner*.

Si vous pouviez développer un peu, parce que je crains qu'on ne franchisse la ligne jaune.

Eric FREUDENREICH

Pourquoi le *Fraud Examiner* s'appelle-t-il, en français, « expert légiste » ? C'est parce qu'il a un rôle judiciaire. Il est l'interface avec les autorités judiciaires, soit du côté de la défense, soit du côté de l'accusation.

Il ne s'agit pas forcément d'imputer, mais de définir qui sont les auteurs, ou bien où sont les responsabilités, si vous préférez cette dernière formulation. On est bien d'accord sur le fait que tout ce que peut faire l'auditeur interne ce sont des recommandations. Ce n'est pas lui qui va délimiter la qualification pénale, je pense que c'est le rôle du juriste. Il ne faut même pas, dans une investigation, penser pouvoir court-circuiter le directeur juridique, parce que c'est lui qui décidera d'abord si l'affaire mérite d'être poursuivie ou pas, et qui décidera aussi, en utilisant peut-être lui-même ses propres conseils, quelles sont les qualifications pénales à retenir parce qu'effectivement, si c'est la mauvaise qualification pénale qui est retenue, les chances de poursuite seront anéanties.

L'INVESTIGATION INFORMATISEE DES FRAUDES : APPROCHES INFORMATIQUES ET CAS PRATIQUES

Pascal GADEA, *Directeur Commercial Grands Comptes France, ACL*

Noël PONS, *Consultant*

Yoanna PONS, *Auditeur S.I., Audéa*

Pascal GADEA

Commençons par le sujet de l'analyse des données. A quoi sert –elle ?

Les enjeux, pour vous, sont d'apprendre à mieux cohabiter avec votre direction informatique, dans le cadre de la lutte antifraude, et à dialoguer en interne en ce qui concerne l'accès à vos données. Sans mettre en cause la sincérité des personnes de l'entreprise, on s'approprie le système d'information et l'on vérifie que ce système d'information est cohérent avec les déclarations qui peuvent être faites par ailleurs avec des systèmes d'évaluation de contrôle interne.

Une des premières raisons est de pallier certaines faiblesses dans les environnements de contrôle interne. On part du principe que ce n'est pas forcément l'audit interne qui est responsable de tout, et qu'il faut rechercher comment les opérationnels peuvent s'approprier un peu mieux leur système d'information, comment les mêmes opérationnels peuvent être un peu plus actifs, et notamment à l'égard des anomalies ou des erreurs dans les SI, pouvant masquer une fraude.

L'idée n'est pas de travailler uniquement sur un mode déclaratif de votre système de contrôle interne, mais c'est de commencer à mettre en place des contrôles dans votre SI.

Pouvoir examiner 100 % des transactions d'une entreprise, c'est possible. Dans certains cas, plus on sera exhaustif et plus l'entreprise sera importante en taille et en volume, et mieux on pourra détecter certaines anomalies. Ce qui est intéressant à ce niveau-là, quand on commence à examiner 100 % des transactions, c'est aussi de pouvoir faire des croisements, et de comparer des données. Les enjeux de l'analyse de données sont aussi de pouvoir exécuter des contrôles et de vérifier l'intégrité des transactions.

Dans l'audit interne, je distingue deux populations d'auditeurs : ceux qui vont adhérer à la technologie et ceux qui n'y adhèreront jamais. Pourquoi n'adhère-t-on pas à une technologie de type ACL ou autre ? C'est tout simplement que l'on ne comprend pas ce qu'est une donnée. Le problème vient souvent de là. Si l'on commençait, indépendamment de la technologie, un apprentissage sur la donnée, qu'elle soit caractère, numérique ou date… et, en fonction de la qualité de cette donnée, le type de contrôle, de filtre à appliquer, si l'on intégrait bien ces basiques, il n'y aurait pas de problème, car la technologie en soi reste assez simple.

On va voir comment ce type de technologie peut se « démocratiser » par rapport à ces défis que sont l'analyse de données et la vérification de l'intégrité des transactions. L'intégrité de ces transactions, on peut s'en assurer en observant la cohérence des montants, les chiffres ronds, par exemple, qui sembleraient aberrants, ou les petits montants sur les notes de frais.

Les enjeux sont d'automatiser des tests appliqués à des zones sensibles dans l'entreprise pour identifier la fraude avant un impact financier important. Ce type d'automatisation des tests peut être de l'audit continu, mais aussi du contrôle continu, dans le sens où on pourrait imaginer, par recommandation du service d'audit interne, de mettre en place ce type de batterie de tests pour les opérationnels, dans les directions financières, logistiques ou opérationnelles. Je pense notamment à la grande distribution.

Mieux comprendre l'analyse de vos logs générés par l'ensemble de vos applications. Je ne vais pas rentrer dans un débat lié à la CNIL, mais on a des retours d'expérience intéressants sur les ID machines ou les identifiants, de manière un peu anonyme, mais qui permettent des vérifications : en couplant 16 applications différentes, en récupérant les logs de chaque application, on peut par exemple voir qu'un prestataire de service informatique externe à l'entreprise qui est sur site depuis 6 mois a tenté 47 fois dans une journée de connecter un système comptable. Il existe des pare-feu qui peuvent émettre des systèmes de *reporting*, qui vous donnent la liste des sites interdits, et des personnes qui ont tenté de se connecter, etc. Et il s'avère que l'on voit encore des entreprises qui nous expliquent que, pour certains pare-feu, il y a une zone d'ombre qui rend possible l'accès à des systèmes, des sites externes à l'entreprise. Je connais des sociétés partenaires d'ACL, notamment, qui utilisent notre technologie auprès de grandes banques pour dire : « Voilà l'ensemble des intrusions que vous avez pu subir. » Pourquoi ? Parce que l'on a pris l'exhaustivité des flux et que l'on a mis en place des contrôles bien précis.

Ce n'est qu'une technologie qui permet de chercher des données. Encore faut-il savoir ce que l'on cherche. Je crois donc qu'il est très important de s'appuyer sur de l'expertise, sur des gens qui peuvent effectivement vous aider, vous orienter. Il peut s'agir des *Big 4*, de cabinets indépendants… Je pense qu'il faut avant tout définir une méthodologie de contrôle avant d'utiliser une technologie.

La piste d'audit peut vous aider à démontrer la fraude.

Historiquement, on peut imaginer qu'un auditeur travaille dans son coin avec un PC portable. On lui extrait des données du SI et il analyse les données. C'est une vision un peu ancienne du contrôle. L'idée ici est d'aller un peu plus loin et de se dire que l'on pourrait avoir une vision partagée du contrôle avec une orientation équipe d'audit. On va donc opter pour un audit continu, en introduisant certains tests automatisés qui restitueront des résultats. Et la mission sera orientée en fonction de ces résultats. Dans ces types de contrôles, on peut imaginer des contrôles à connotation antifraude, notamment sur la paie, sur les notes de frais, sur des sujets liés à la comptabilité, aux entrées dans le journal. Il y a des choses que l'on peut expliquer. C'est vrai que quand on étudie les entrées dans le journal, cela peut être dans les périodes de clôture, avec une forte montée en charge. Et on peut trouver des exemples de quelqu'un qui a fait des entrées dans le journal, ou des sujets délicats comme les modifications manuelles dans un système d'information, et qu'il faut documenter.

Peut-être une personne a-t-elle utilisé son PC pour effectuer une saisie alors que, en faisant un croisement avec son fichier congés, on se rendrait compte qu'elle n'était théoriquement pas dans l'entreprise depuis trois semaines. C'est peut-être une personne qui, par inadvertance, a laissé son *User Password* à son assistante. Cela peut valoir une recommandation et un rappel à l'ordre. Ou alors c'est quelque chose de beaucoup plus grave.

Le fait de croiser et d'avoir ainsi des équipes qui pourraient se partager ces contrôles permet d'aider certains auditeurs plus experts à former les néophytes, ceux-ci utilisant des contrôles préfabriqués par ceux-là, ce qui les aidera dans leurs investigations. On peut imaginer une approche à l'échelle de l'entreprise, qui est de dire que le contrôle et la lutte antifraude, c'est l'affaire de tous, avec un bon plan de communication interne. On pourrait tout simplement imaginer que ce type de technologie puisse remonter des alertes ; on peut aussi imaginer des contrôles complètement automatisés et qui délivreront des résultats.

En résumé, **la technologie doit vous permettre de pouvoir travailler sur vos données en mode lecture uniquement**. Il ne faut surtout pas que la technologie vous permette de modifier les données de l'entreprise.

Il faut pouvoir importer un grand nombre de formats de données. Il y a, dans l'Administration publique, de très grandes administrations qui nous utilisent pour faire des contrôles qui peuvent être à connotation fiscale, comme l'URSSAF ou les douanes. Pourquoi ? Parce que, dans ce type de technologie, on va importer des formats type PDF, fichier d'impression. On va se connecter à un

mainframe, se connecter à SAP. On va comme cela croiser tous types de formats de données ou bien récupérer la table des logs, de tous les logs du marché, parce que ce sont des fichiers plats, qui sont structurés. Au départ, je n'y croyais pas. Grâce à un grand assureur français j'ai eu la confirmation que cela fonctionnait.

Il faut gérer la totalité de vos données : il n'y a donc pas de limite en volumétrie. Le plus gros fichier que l'on ait traité en France, pour la Cour des comptes, c'est la paie des fonctionnaires : 945 millions de lignes, 30 colonnes.

Il faut utiliser des fonctions simples pour analyser vos données, et effectuer des correspondances entre différents systèmes d'information ; automatiser tous vos contrôles et mettre en place une gestion simple des alertes.

Quelques exemples d'application. La gestion des stocks : analyse des mouvements, régularisations d'inventaires, rectifications manuelles de stocks, contrôles des démarques. Les notes de frais : soumettre une même dépense deux fois, identifier les seuils ou montants excessifs, vérifier la cohérence des montants de voyages par rapport à la distance et au moyen de transport utilisé. L'analyse des logs de connexion : analyse des logs système, des tentatives d'intrusion, des connexions distantes. La séparation des tâches : analyse des droits des utilisateurs, des mots de passe, des traces utilisateurs. Il y a beaucoup à faire dans le domaine de la séparation des tâches.

Il faut commencer doucement sur l'investigation de fraude dans les données : un petit périmètre, un petit processus. Avec l'expérience, petit à petit, vous commencez à élargir le processus et l'investigation des données sur d'autres processus. Illustration : on voit ce que l'on peut faire avec une simple interface web. On imagine qu'un utilisateur, un auditeur par exemple, va se connecter à un environnement de contrôle. En fonction de son profil, il va voir une gestion de documents – des documents Word, PDF, de bonnes pratiques, les documents de l'IFACI, des rappels, etc. Il peut ensuite tout simplement aller sur la partie que l'on appelle analytique dans l'interface (*AX Gateway*, chez ACL), qui est l'interface web, et de voir par exemple un ensemble de contrôles : sur les noms approchants, les montants incorrects, les montants au dollar près ; un ensemble de contrôles qu'il peut utiliser et exécuter. Il choisit un des contrôles, il entre certains paramètres et s'intéressera à tel type de contrôle. Il pourra ouvrir le fichier Excel, l'imprimer dans son rapport, dans sa recommandation, ou alors partir avec et demander les 100 pièces justificatives de ces 100 lignes-là, si ce sont des notes de frais ou des factures, par exemple.

Il y a toujours une trace des recherches : ce résultat, je l'ai obtenu par telle personne, à telle heure, qui a lancé tel contrôle.

Autres exemples : un doublon de paiements ou une alerte. On peut notamment alerter des responsables de processus avec une simple interface web. Imaginons que je reçois un e-mail qui me dit de me connecter, parce que les doublons dont on vient de parler, je les ai reçus également. Je me connecte et là, je suis patron d'un processus qui est *Payment Duplicate*, qui est tout le processus achats. Je vois que j'ai des alertes. Je vais voir à quoi cela correspond dans mon système d'information. Ce sont des lignes qui sont peut-être extraites de 30 millions de lignes. Ces lignes-là, a priori, me posent problème. L'idée est de pouvoir choisir une partie de ces lignes et de les affecter à mes collaborateurs – c'est la notion de *workflow* – en y ajoutant mes commentaires. Un de mes collaborateurs a maintenant des alertes qui lui sont assignées. Au moment où je sauvegarde ce que je viens de faire, mon collaborateur se connecte, et il reçoit un e-mail qui lui dit de se connecter. Il se connecte et il voit des alertes, et mes commentaires qu'il peut compléter. On peut comme cela avoir tout un ensemble de commentaires qui sont toujours auditables.

Si, dans six mois, vous vous rendez compte que les doublons ou les incohérences sont toujours apparentes dans le système d'information, c'est le moment de vérifier l'efficacité du contrôle en interne.

Comment devenir proactif dans la gestion de la fraude ?

On ne peut bien sûr pas tout contrôler, mais le but est de montrer qu'il y a un réel effort de mettre en place une technologie assez simple pour le faire ; de pouvoir automatiser, d'avoir une notion de récurrence des analyses ; et, d'une manière assez immédiate, de détecter toute anomalie, pouvant être liée à une fraude ou tout simplement à une erreur de gestion.

Mettre en place un environnement de contrôle sera apprécié par votre direction générale, le comité d'audit, voire vos CAC qui connaissent bien ce type de plateforme.

Noël PONS

Qu'est-ce que la fraude ? « Tout acte illégal, caractérisé par la tromperie, la dissimulation ou la violation de la confiance. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial. »

Quel est son impact dans une société ? Il peut être nul, mineur ou majeur. Dans certains cas, des petites fraudes, faciles, connues, parce qu'elles adviennent au plus mauvais moment, dans une situation particulière, peuvent être mortelles. Des fraudes plus importantes peuvent ne pas avoir de conséquences immédiates graves. Quels secteurs affecte-t-elle ? Tous. On ne peut pas savoir quel est le secteur le plus vulnérable. Qui sont les fraudeurs ? Peut-être vous, moi, on ne sait pas. La fraude est tellement liée à l'humain que chacune des situations est particulière. C'est le fraudeur qui dispose !

Cela fait beaucoup de points d'interrogation. Dans cet environnement, l'analyse du risque est le début de la sagesse.

L'état des lieux, aujourd'hui. Pour des gens qui s'intéressent à la fraude, disons que c'est la belle vie. En effet, les crises font remonter à la surface des montages anciens et créent de nouveaux systèmes adaptés à l'avancée technique. Nous sommes actuellement dans les Ponzi verts. Qu'est-ce que c'est ? Ce sont des « Madoff » adaptés à l'écologie. Si vous observez un relevé de société, vous constatez qu'une multitude d'entre elles sont *green*. Tout le monde est vert. Des démarcheurs proposent entre autres des systèmes de fabrication de carburant à partir d'eau de plantes etc. ; cette escroquerie fonctionne depuis 1902.

Désormais, les plus grandes fraudes identifiées sont essentiellement des délits d'initiés, opérations extrêmement complexes, dont la recherche ne peut se faire manuellement.

Yoanna PONS

Pour élaborer un cadre de recherche de la fraude, il faut d'abord savoir ce que l'on cherche.

Chaque type de fraude présente des caractéristiques bien spécifiques auxquelles on ne peut déroger. Par exemple, un fraudeur qui décide d'encaisser des montants détournés va devoir soit créer un RIB, soit en modifier un. C'est un passage obligatoire.

Si les types de fraude commencent à être connus par tous, ce sont plutôt les montages ou les moyens utilisés pour frauder qui sont encore laissés au choix du fraudeur – et ils sont spécifiques à chaque entreprise –, ainsi que les nouvelles technologies qui donnent la possibilité aux fraudeurs d'aller de plus en plus loin, et surtout de frauder de plus en plus rapidement.

Une fois que l'on a établi ce que l'on cherchait, il faut savoir où et comment le chercher. Ces deux notions relèvent de la cartographie des risques qui doit être établie.

Il faudra établir un relevé des logiciels que l'entreprise utilise, dresser le circuit des transferts des données établi dans l'entreprise, les modifications intervenues au cours des années d'utilisation de

ces logiciels, mais surtout analyser le cadre de séparation des fonctions et les seuils fixés par l'entreprise.

Une fois récoltées toutes ces données, il faut le faire savoir au sein de l'entreprise. Savoir le faire savoir est une donnée très importante et en même temps très compliquée, parce que c'est une notion qui relève logiquement de la communication de crise. On remarque qu'en général, dans une entreprise, quand on commence à parler de lutte contre la fraude, les réactions sont très diverses. Certains pensent que c'est normal et logique d'en parler, d'autres ne se sentent pas concernés et pensent que cela n'arrive que chez les autres.

Noël PONS

Il est nécessaire, avant tout, de constituer un historique des montages qui ont antérieurement affecté l'entreprise. Ces derniers sont, dans la majorité des cas, systématiquement réutilisés. Il faut créer une veille sur les risques nouveaux ; puisque tout évolue, des adaptations de montages anciens auront lieu qui vont s'installer sur une base nouvelle. Et enfin, il faut disposer d'une base méthodologique.

On va vous présenter ici un exemple qui est le couteau suisse de la fraude. Vous l'avez tous rencontré. Si vous me dites que c'est faux, je ne vous croirai pas. Il s'agit du fractionnement des opérations.

Couteau suisse, pourquoi ? Parce que cela affecte les manipulations dans le secteur privé, dans les liens entre entreprises, fournisseurs et clients, et dans le secteur public, les marchés publics sont particulièrement touchés. Cela facilite les fraudes internes et/ou la corruption, dans le cadre des autorisations d'engagement, des remises ou encore des limites fixées aux *traders*, ou autres opérations.

Quels sont les invariants ? Le livre d'achats, les comptes fournisseurs, les paiements et tant d'autres éléments permettant des tris : dates, lieux, montants, fournisseurs. On est déjà ici dans la préparation de la méthodologie et de la preuve.

Le fractionnement est un montage qui n'attire pas l'attention du néophyte parce que le processus est organisé : l'autorisation est fixée à, 40 000 euros ; l'auditeur relève une facture de 39 000 euros. Tout semble normal. Par contre, si 25 factures à 39 000 sont relevées, un tout autre problème se pose, surtout si le même fournisseur est concerné.

Yoanna PONS

Pour entrer dans le détail, choisissons des fichiers dans lesquels on ira chercher l'information. Nous avons choisi le fichier maître fournisseurs et le fichier des paiements. Nous avons fait ce choix parce qu'on a voulu toucher le plus grand nombre d'entreprises, ONG comprises. Dans chaque entreprise, il existera sûrement des fichiers beaucoup plus pertinents pour cette analyse. En matière de fraude, il ne faut jamais oublier que toute fraude doit toujours être adaptée aux spécificités de l'entreprise. Chaque entreprise doit se l'approprier, parce qu'elle est propriétaire de ses données. Et c'est évidemment elle-même qui connaît le mieux sa façon de fonctionner.

Pour rechercher une fraude, deux étapes sont établies. La première étape est la recherche d'atypismes, d'erreurs, de possibles fraudes. Dans ces cas-là, on utilisera des fonctions données par les logiciels. Par exemple, dans une recherche de doublons, on va s'intéresser à la fonction de stratification sur les montants des factures avec une limite de $\pm$ 5 % des montants.

C'est une entreprise qui établira un contrôle de double signatures pour toutes les factures supérieures à 10 000 euros. Grâce à ce logiciel, on cherchera toutes les factures qui se trouvent entre 9 500 euros et 10 000 euros. On analysera les situations au cas par cas pour valider le respect de ces

principes. Dans certains cas, on constatera que, dans le lot, il existe des factures présentant des caractéristiques communes, qui sont répétitives et qui, soulèvent donc un léger doute , donnant lieu au passage à une seconde étape qui consistera à approfondir l'analyse de tous ces atypismes.

Le fait d'utiliser des logiciels d'extraction a une très grande importance parce que, à partir du moment où les atypismes sont découverts, on dispose d'un début de preuve. Une fois que cette démarche a été faite, on va pouvoir s'intéresser à tel atypisme, savoir s'il s'agit d'une exception. En réalité, il se justifie souvent, c'est un cas particulier, parce que, de temps en temps, avec tel fournisseur, il nous arrive de fractionner les factures ; Lorsque rien n'est expliqué, lorsque rien n'est prévu dans le contrat, lorsque des rapprochements qui ne sont pas logiques ne sont pas prévus, on ira alors beaucoup plus loin à partir de ce premier tri qui est exhaustif.

Il ne faut pas croire qu'une seule façon et une seule utilisation sont applicables par type de fraude. Une même recherche de fraude peut être menée de façon totalement différente.

Intéressons nous au fichier des paiements mais, au lieu d'utiliser la fonction de stratification, on va utiliser la fonction totaliser ou classer, en fonction des cas et en fonction des champs. Pour parer à l'ingéniosité des fraudeurs qui, ayant eu connaissance du fait que toutes les factures qui étaient juste au-dessous du seuil de contrôle étaient vérifiées – ou du moins une bonne partie –, vont se dire : « Dans ce cas-là, au lieu de faire une facture qui sera juste au-dessous, on va faire une facture mais on va la diviser en 2, en 3 ou beaucoup plus. » En divisant ces montants, les faux ne seront plus du tout dans ce seuil de contrôle. Et c'est tout l'intérêt d'utiliser ces fonctions-là puisque, une fois réunies, parce qu'elles ont des caractéristiques identiques, *elles vont dépasser ce seuil et même, dans certains cas, être vraiment très supérieures à ce seuil, sans qu'aucun contrôle n'ait été effectué pour ces factures.*

Dans ce cas-précis, l'investigation sera approfondie, en allant chercher, par rapport à ce début de preuve, et en établissant des concordances par rapport à des fournisseurs, à des acheteurs ; par rapport à des produits en particulier, à des prestations ; mais également par rapport à un secteur géographique. Pour pouvoir identifier cette récurrence ou le côté systémique qui, une fois démontré, va nous permettre de mettre en avant la nature volontaire de la manipulation. Cette manipulation des fichiers étant sanctionnable pénalement par l'article L.323-3 du code pénal.

Noël PONS

Pour prévenir ce type de fraude il faut d'abord une séparation des fonctions solide et réelle, avec des remontées d'informations pertinentes. Ensuite, un suivi des atypismes, et une analyse approfondie de tout ce que l'on ne comprend pas. Plus généralement, une organisation dédiée ou habilitée pour gérer l'ensemble des problèmes relatifs aux fraudes est préconisée.

Quelles leçons doit-on en tirer ? Premièrement, douter de tout. Se poser la bonne question au bon moment

Yoanna PONS

Deuxièmement, tenir constamment à jour la cartographie des risques, car les montages les plus simples sont malheureusement les plus efficaces. La cartographie est à la base de la recherche que l'on veut établir, et elle doit être tenue à jour en fonction de tous les moyens dont dispose un fraudeur.

Noël PONS

Comment devenir proactif dans la gestion de la fraude ?

Cette cartographie des risques est relativement récurrente. Dans ma vie – je travaille sur ce sujet depuis 1972 –, j'ai vu environ 1 800 cas de fraude, qui se réduisent à une vingtaine de typologies. En fin de compte, c'est toujours le même montage que l'on retrouve.

Savoir ce que l'on cherche, où on le cherche et comment aller le chercher.

Yoanna PONS

Disposer des ressources nécessaires pour prévenir les fraudes.

Noël PONS

Savoir prendre le temps pour examiner tous les détails. Le diable se cache dans les détails, et c'est là que l'on perd le plus de temps et que l'on rencontre le plus de problèmes.

Yoanna PONS

Et bien évidemment, savoir le faire savoir. Le fait de présenter à toute son entreprise les contrôles qui sont mis en place, et d'annoncer le fait que la lutte contre la fraude est engagée est la base de la prévention qui doit être mise en place au sein d'une entreprise.

QUESTIONS/REPONSES

Question de la salle

Merci pour cet exposé très clair. Est-ce que le fait de « savoir le faire savoir », ne risque pas d'être à double tranchant à l'égard de potentiels fraudeurs ? En leur expliquant nos méthodes de contrôle pour chercher la fraude, ne risque-t-on pas de leur donner des idées ?

Noël PONS

Bien sûr, il y a un risque. 20 % des gens frauderont toujours ; 20 % des gens ne frauderont jamais ; 60 % peuvent basculer du mauvais côté. L'essentiel est la clé que l'on va laisser au fraudeur. Si l'on dit au fraudeur qu'il y a une fraude parce que le modèle marche mal, et s'il n'a pas accès au modèle, il pourra toujours s'agiter, il n'y arrivera pas.

Le problème est de prévenir les 60 % qui risqueraient de basculer, et de faire en sorte de n'avoir plus que le noyau dur des fraudeurs à gérer, ce qui peut être déjà suffisamment grave. Cela a été un sujet qui a fait l'objet de longues discussions avec Louis Vaurs, en 2004, lorsque « Audit et fraude a été édité avec François VIDAUX. Tout tient à cette couverture, si on sauve 80 % de la tentation de fraude, on a gagné.

C'est un risque à prendre, de toute façon. Mais si les contrôles sont en place, le risque est partiellement maîtrisé.

Question de la salle

Si j'ai bien compris, vous disiez que l'on pouvait classer les fraudes dans une vingtaine de typologies. Pouvez-vous en citer ? Cette liste doit être connue.

Comment devenir proactif dans la gestion de la fraude ?

Noël PONS

C'est le moment intéressant de l'analyse de la fraude. On passe du montage à l'humain. C'est un vieux chiffre qui date de 1973 et qui n'a jamais été remis en cause. Alors, c'est peut-être 15, c'est peut-être 18, c'est peut-être 25, je ne sais pas ; et selon les pays et les contrôles mis en place, cela peut varier. Il faut savoir que environ 30% ou 40% des pays sont à peu près sous contrôle – il y a des fraudes, mais on les contrôle – et que, pour les autres pays, on s'aperçoit de la fraude quand elle est réalisée. Aucun contrôle n'existe.

Dans une structure contrôlée, on connait le profil des fraudeurs, celui qui veut s'enrichir absolument. Celui dont le fils a un problème de santé, et pour lequel une opération est nécessaire aux États-Unis : Il gère les stocks, il va trouver les 500.000 euro nécessaires. Il y a les joueurs, les parieurs, etc. et un pourcentage récurrent de tentatives.

On est là sur de l'humain pur. C'est d'ailleurs tout l'intérêt de la fraude : on a en face de soi un homme ou une femme, enfin quelqu'un.

COMMENT DEVENIR PROACTIF DANS LA PREVENTION ET LA DETECTION DE LA FRAUDE ?

Bernard DECOEUR, *Chargé de Mission, Direction Audit & Risques, Service du Contrôle Interne GDF SUEZ*

Emmanuel PASCAL, *Audit Manager, Brakes Group*

Hugh PENRI-WILLIAMS, *Administrateur, ACFE Chapitre France*

Bernard DECOEUR

Nous interviendrons en trois temps. Je vous présenterai le premier volet, qui est l'existence d'une politique antifraude. Ensuite, Hugh PENRI-WILLIAMS parlera du dispositif de prévention. Enfin, Emmanuel PASCAL traitera l'existence d'un dispositif de détection.

Ces trois points seront traités sans pudeur excessive ni curiosité malsaine.

L'**existence d'une politique antifraude** implique fondamentalement un **engagement fort des dirigeants**. Sans engagement fort des dirigeants, une politique de prévention ou de détection de fraude aura du mal à aboutir. Et le premier symbole de cet engagement est une définition de la fraude.

Vous noterez que cette définition est un peu plus large que celle que nous a présentée Noël Pons il y a quelques instants, puisqu'on y a inclus les entorses aux règles de l'organisation. Je la lis rapidement : « La fraude consiste à tromper délibérément autrui pour obtenir un bénéfice illégitime ou pour contourner des obligations légales ou des règles de l'organisation. Un comportement frauduleux suppose donc un élément factuel et intentionnel, ainsi qu'un procédé de dissimulation de l'agissement non autorisé. »

Quatre piliers sous-tendent en fait cette définition. Le premier, un élément intentionnel : pas de fraude sans intention. Un acte matériel illégitime, bien évidemment : par là, on vise effectivement notamment les entorses aux règles ou aux lois, mais également les entorses aux règles que s'est données l'organisation. Une recherche de bénéfices, matériels ou non, pécuniaires ou non ; la reconnaissance fait partie de certaines motivations de fraudeurs. Et un acteur qui peut être au sein de l'organisation ou en dehors de l'organisation.

Dans ce contexte-là, la fraude peut prendre différentes formes, dont certaines ont une qualification pénale. Je n'en listerai que quelques-unes : la corruption, le vol, le détournement de fonds, les faux en écriture, les contrefaçons, l'escroquerie, le blanchiment d'argent, les fausses déclarations, les dissimulations de données, etc.

Au-delà de la définition d'une politique, il y a nécessité de prendre des **mesures qui confortent cet engagement**. Ces mesures peuvent encore une fois revêtir différentes formes. Nous en avons identifiées un certain nombre.

La première, qui est un symbole fort, ce sont des valeurs affirmées. Cela peut faire sourire, dans un premier temps, mais ce sont les règles du jeu et les points forts identifiés par l'entreprise ou l'organisation qui doivent sous-tendre les actes de chacun.

Des guides de bonnes pratiques : on retrouve cette démarche dans un certain nombre d'organisations. Guides de bonnes pratiques concernant par exemple les acheteurs, les commerciaux.

Des mises en situation avec des éléments de réponse diffusés et portés. Je pense notamment aux cadeaux d'entreprise, à la prise en compte de l'aspect culturel : recevoir un cadeau, en Chine, ce n'est pas tout à fait la même chose que de recevoir un cadeau en Allemagne.

Une organisation et des responsabilités affichées. Il faut non seulement que les règles du jeu soient définies, mais il faut qu'au-delà, l'organisation soit lisible, que l'on sache qui fait quoi et, dans ce contexte-là, que les délégations de pouvoirs soient formalisées et connues. C'est un point très important, notamment dans le cadre de réorganisations, de modifications de périmètres de responsabilités.

Il serait malvenu de ne pas évoquer un **environnement de contrôle sain**. Un comportement exemplaire des dirigeants. Autrement dit, faire ce que l'on dit. Des décisions cohérentes, c'est-à-dire en ligne avec les valeurs prônées par l'entreprise et les règles du jeu que s'est donnée l'organisation.

Pour prendre un exemple tout simple, on peut crier haut et fort que la fraude est quelque chose de condamnable, si à la première fraude, il n'y a pas de sanction, tout message deviendra peu crédible.

Une sensibilité aux signaux faibles : à l'image d'ailleurs de la sécurité industrielle, un certain nombre de dérives ponctuelles, marginales, peuvent, avec le temps, prendre une dimension beaucoup plus organisée, qui peuvent à la limite traduire la mise en œuvre d'un véritable réseau de fraudes.

Il nous a donc semblé important d'insister sur ce point-là et, en écho, de faire référence au triangle de la fraude qui est un mécanisme bien connu : motivation, opportunité, rationalisation. Autrement dit, un défaut de contrôle, une pression extrêmement forte, notamment dans le cadre des objectifs, et un sentiment d'injustice vécu par tel ou tel sur une promotion qu'il estimait raisonnable d'obtenir, font que cette personne fait partie des 60 %, dont parlait Noël Pons tout à l'heure, qui peuvent, du jour au lendemain basculer dans le domaine de la fraude.

Une **panoplie d'outils** : on a retenu la nécessité d'avoir un état des lieux de l'organisation, qui repose sur huit incontournables : définition des responsabilités ; organes de gouvernance impliqués et informés (qui fait quoi) ; politique antifraude formalisée et mise en œuvre ; cartographie des risques de fraude ; ressources affectées aux enjeux ; système de contrôle interne opérationnel ; rôle de l'audit interne défini ; traitement efficace de la fraude.

Ces incontournables sont déclinés en pratiques observables. Chaque pratique est évaluée à l'aide d'une grille à trois niveaux : un niveau que l'on considère comme indispensable ; un niveau que l'on considère comme souhaitable ; et un niveau que l'on considère comme contributif à la détection et à la prévention de la fraude.

Cette panoplie d'outils s'appuie – on y a fait référence – sur une cartographie des risques en général ; des contrôles internes adaptés ; une organisation pertinente (modalités d'investigation, cellule de gestion de crise, communication ad hoc) ; des modalités d'investigation définies (identification des acteurs clés).

Hugh PENRI-WILLIAMS

Noël Pons m'a volé la vedette, à propos des anges et des démons. Je serais un peu plus prudent que lui. 5-10 % des employés sont des gens strictement honnêtes. 5-10% ont l'intention de voler avec préméditation. 80-90% peuvent commettre des fraudes si les circonstances sont réunies. Mais cela bouge beaucoup, d'un pays à l'autre, d'une région à l'autre, d'un métier à l'autre.

J'ai travaillé dans l'assurance, pendant une quinzaine d'années ; c'est un métier où la fraude est très répandue, surtout par les assurés, mais aussi à l'intérieur de l'entreprise.

Il y a des gens dont la seule intention, quand ils achètent une police d'assurance, c'est de frauder. C'est un investissement de leur part, de payer leur prime. Et ils ont parfois plusieurs polices.

Comment devenir proactif dans la gestion de la fraude ?

Dans la situation de prévention, pour éviter que les 90 % de personnes « indécises » aillent vers le côté noir, il y a plusieurs moyens.

Si la prévention n'est pas faite dans certaines règles de l'art, il y a un danger qui est de dépasser nos pouvoirs : la fin ne justifie pas les moyens. Cela doit être toujours présent à l'esprit de tous les acteurs, lesquels devraient recevoir une formation spécifique pour agir en toute légalité mais avec efficacité et rapidité.

Les auditeurs internes savent qu'ils doivent respecter la confidentialité ; protéger les documents et les relations d'entretiens. Selon moi, leur rôle est celui d'un rôle d'un juge d'instruction. Ils ne sont pas seulement à charge, mais aussi à décharge. Ils ne sont pas là seulement pour trouver les preuves contre quelqu'un ou contre un groupe de personnes, mais aussi les preuves pour les disculper. Les néophytes, les novices peuvent avoir tendance à aller trop loin, et à pratiquer la chasse à l'homme. C'est très dangereux. Et j'insiste sur ce point. L'investigation de fraude, mal conduite, peut se retourner contre vous et votre service d'audit.

D'autres choses sont à ne jamais faire : se livrer trop facilement au premier soupçon, aux impressions ; commencer une investigation sans consultation ni autorisation ; mentionner les noms dans les rapports ; accuser quelqu'un personnellement, surtout devant des témoins ; interviewer quelqu'un seul ; fouiller dans les affaires personnelles de quelqu'un ou l'empêcher de quitter les lieux. Si vous ignorez ces points, vous pouvez vous-même être accusés de l'une ou de l'autre des infractions à la place du suspect principal !

Une règle d'or est la préparation. Il est naturel, dès qu'une affaire vient sur la table, de dire : « Nous devons aller vite pour confronter les gens, pour les interviewer. » Pas du tout. Il est nécessaire de préparer sa mission, sans mettre au jour ce que l'on est en train de faire. Le plus grand danger pour nous est que la direction générale envoie sur l'intranet une communication : « Nous sommes en train de poursuivre quelqu'un pour ceci ou cela. » Cela ne nous aide pas du tout. Il est parfois nécessaire de dire à la direction générale : « Laissez-nous travailler, constituer une cellule de crise, déterminer tous les aspects. Et après un certain temps, dès que nous aurons assez de preuves, soit pour, soit contre, nous commencerons à interroger les gens potentiellement impliqués, mais pas tout au début. » On doit se freiner.

Dans le cadre du dispositif de prévention, vous pouvez créer un site sur votre intranet pour aider à mieux connaître la fraude : documentation interne, procédures, description de cas de fraude, sources externes disponibles sur le sujet, etc. C'est facile à mettre en œuvre.

Le *Continuous Auditing* est un concept que, personnellement, je n'ai pas vraiment pratiqué. Mais vous pouvez l'utiliser, surtout avec des outils comme ACL. Vous pouvez mettre un dispositif en place qui tourne constamment dans vos systèmes informatiques pour vous alerter, en dehors des missions ponctuelles de l'audit interne. Pour moi, c'est au contrôle interne de gérer cela, pas à l'audit interne, mais cela dépend de votre organisation. Quoiqu'il en soit, cela peut vous aider à détecter des anomalies, et à limiter les dégâts.

Une autre technique préconisée par l'IIA est le *Control self-assessment* ou *Risk & Control self-assessment*. C'est une façon structurée de mettre en garde contre les risques de la fraude les différents métiers.

Je passe maintenant la parole à Emmanuel, qui va nous expliquer l'intégration des contrôles dans l'audit.

Emmanuel PASCAL

Pour prendre en compte le risque de fraude dans tous les audits, il faut, premièrement, **dépasser le stade de l'assurance**.

Savoir profiter des avantages offerts par l'informatique en allant tester l'ensemble des données et certaines données nouvelles ; élargir le champ des contrôles à des domaines moins couverts en prenant en compte l'historique ou l'environnement ; aller au-delà des schémas classiques en imaginant des scénarios plus complexes qui croiseraient plusieurs processus ; et ne pas oublier les cas classiques de fraude.

Il faut, deuxièmement, **tester le risque en réel**, pour que le management en prenne conscience.

Ne pas se fonder sur l'historique mais sur le futur ; faire intervenir tous les acteurs des processus dans leur quotidien ; prendre des précautions avant (en interne ou en externe), car le test doit être géré comme un projet ; introduire des faux documents (factures, commandes, contrats…) ; simuler des fraudes informatiques.

Je vais maintenant vous parler du **dispositif de détection**. Selon une étude de l'ACFE (sur base mondiale), les dispositifs de détection classiques couvrent moins de 50% des cas. Les fraudes identifiées grâce à l'audit interne sont de 14% ; 5% pour l'audit externe ; les fraudes identifiées grâce au dispositif de détection de l'entreprise sont de l'ordre de 30%.

Les **difficultés de la détection** : ce sont les fraudes sur des petits montants. On ne les verra pas forcément puisqu'ils sont au-dessous des seuils. Il y a des schémas complexes ; il y a aussi des schémas simples. Mais il ne faut pas croire que tout le monde passe par une société écran.

Autre difficulté, les événements isolés dans le temps. Si vous faites un audit sur le mois de mars et que vous vous concentrez sur ce seul mois, vous ne verrez pas les fraudes commises dans les autres périodes. C'est le fameux problème des volumes que l'on devrait normalement pouvoir gérer avec certains logiciels.

Les **limites de la détection.** Ce sont d'abord les accès aux informations limités par la législation ; ce sont les remontées des informations règlementées ; ce sont les risques sur l'image de la société.

La détection vient des intervenants, et pas seulement des machines. Les opérationnels ne sont pas toujours formés ou disponibles. Tout le monde n'a pas la même vision transversale. En fait, les gens ne voient pas la fraude, ils ne voient pas le mal où il est. On entend des discours du style : « Non, ce n'est pas lui. », « Oh non, pas lui. Moi, j'ai confiance en lui. » ou « Non, ce n'est pas si grave. » Il y a difficulté d'acceptation lorsque des soupçons se portent sur quelqu'un d'insoupçonnable. Donc, certains intervenants risquent de ne pas faire remonter les informations.

Autre problème, le risque de dissimulation du management. Je parle là de la voie hiérarchique. Allez-vous faire remonter l'information selon laquelle votre collaborateur triche, sachant que cela va vous nuire ?

Autre problème encore, la complexité des informations remontées. Il y a les volumes ; il y a aussi les précisions, les détails. On va effectivement vous faire remonter des informations, mais vous n'aurez peut-être pas tout ; ou tout ne sera pas forcément exploitable.

Vous serez amenés à déléguer et donc à former sur les techniques de fraudes. La formation aura trois objectifs : faire prendre conscience ; énoncer les précautions de base ; et former à la connaissance du dispositif de remontée d'informations.

La première des précautions de base est d'être discrets : il faut éviter de tomber brutalement sur quelqu'un. Il vaut mieux éviter certains dérapages.

La formation doit être continue, puisque la fraude est protéiforme.

Les questionnaires de **remontée d'informations** sont un peu une autoformation. Je vais vous faire part d'une expérience que j'ai eue, d'une formation « pour faire peur ». Lors de mon passage dans le secteur public, on a fait une formation pour des responsables RH, en leur disant, sans entrer dans les détails, que l'on contrôlait les heures. On leur a montré très rapidement les contrôles que l'on faisait.

Dans les semaines qui ont suivi, il y a eu beaucoup moins d'heures de nuit, d'heures supplémentaires, etc.

Concernant toujours la remontée des informations, je vais passer rapidement sur le dispositif de *whistleblowing* (en français, « alerte professionnelle »), qui n'est pas exportable en l'état, et qui est un processus assez difficile et assez long. Je vous conseille d'adresser votre projet à la CNIL qui examinera votre demande et donnera (ou ne donnera pas) son accord. Le cadre américain de couverture des salariés n'existe pas en France. Dans notre système, la personne qui ferait remonter l'information ne serait pas protégée. Si le *whistleblowing* est difficile à mettre en place, il ne faut surtout pas oublier le cadre normal hiérarchique de remontée des informations par les managers.

Les **indicateurs**. Il n'y a pas d'indicateur miracle. Nous, dans la distribution, nous avons la chance d'avoir un indicateur qui s'appelle la démarque inconnue, la disparition de stock. Lorsque vous considérez un taux de démarque inconnue, je ne suis pas sûr que vous puissiez l'analyser très facilement, parce que ce n'est pas une information réglementaire ; vous ne la trouvez donc pas dans les rapports annuels des sociétés.

J'ai une technique pour suivre la démarque inconnue : c'est l'analyse volumétrique. Au lieu de parler en argent, je parle en volume aux opérationnels. Je leur dis, par exemple, que, tous les jours, sur leur dépôt, trois palettes sont volées. Cela les impressionne plus qu'une somme d'argent, et les responsabilise davantage. Et je pousse la simulation plus loin : si trois palettes sont sorties, comment se fait-il que personne ne les a vu sortir ? D'autre part, si tous les jours un employé volait un produit, combien cela me coûterait-il ? En émettant des hypothèses, on peut évaluer le taux de démarques inconnues et partant, le risque encouru.

Les **outils de détection**. Si vous croisez les comptes en banque d'une société, pour identifier par exemple les gens qui auraient indiqué leur numéro de compte pour créer des employés fantômes, imaginez ce que vous obtenez lorsque vous croisez tous ces comptes en banque, dans les fichiers du personnel. Ce sont des informations qui concernent la vie privée, et vous n'êtes pas autorisé à disposer de ce genre d'information. Ce sont des croisements dangereux dont il faut se méfier.

L'**audit de fraude** est inclus dans les programmes de travail de l'audit interne. C'est une démarche classique mais plus poussée.

Lorsque vous avez identifié un cas de fraude, l'étape suivante est l'investigation, qui commande d'agir avec beaucoup de précaution.

QUESTIONS/REPONSES

Question de la salle

Vous avez parlé de *whistleblowing*. Mais vous n'avez pas parlé de cette nouvelle loi extraordinaire, de la LME sur la déclaration de soupçon pour le blanchiment.

Emmanuel PASCAL

J'avoue mon ignorance. J'ai travaillé sur la politique de fraude dans ma société, il y a quelques mois, et je me suis concentré sur la CNIL.

Question de la salle

Je voulais savoir si vous aviez des statistiques sur l'efficacité des dispositifs d'alerte professionnelle, en Europe ou en France.

Comment devenir proactif dans la gestion de la fraude ?

Emmanuel PASCAL

Malheureusement non. Mais mon sentiment, c'est que cela ne marche pas très bien. Je pense que, au-delà de tous les clichés, culturellement en France, cela ne marche pas. On ne peut pas changer une culture du jour au lendemain.

Romain MARIE

J'ai fait une étude, dans le CAC 40, sur tous les systèmes de *whistleblowing*. J'ai dû analyser 30 réponses sur 40, environ. Et je vous rejoins effectivement : les résultats étaient assez décevants dans l'ensemble. C'étaient surtout des anomalies de type RH qui étaient remontées. Avec un particularisme sur le système de remontée américain.

Question de la salle

Dans le cadre de vos démarches, je suppose que vous avez dû faire un certain nombre de demandes d'autorisation à la CNIL, en termes de finalité de recherche, de croisement de fichiers, d'exploitation de données, etc.

Avez-vous rencontré quelques difficultés particulières dans l'obtention de ces autorisations de la part de la CNIL ?

Emmanuel PASCAL

C'est assez compliqué. Pour l'instant, nous n'avons pas fait de demande pour les alertes professionnelles à la CNIL.

Sur l'usage des caméras, vous faites votre demande. Les caméras doivent être placées d'une certaine manière. Ces demandes reçoivent un bon accueil de la part de la CNIL.

Pour ce que je vous ai expliqué sur les croisements de fichiers, ce ne sont pas des demandes. Lorsque vous maintenez un fichier, vous devez le déclarer. Mais si vous croisez des fichiers et que vous les détruisez ensuite, vous n'avez pas à les déclarer. Toute la démarche de la CNIL consiste à éviter de ficher les gens.

Pour les fichiers tendancieux, il faut donc faire une demande d'autorisation. Il y a ensuite toute une série de démarches : ces fichiers doivent être détruits au bout d'un moment ; ces fichiers doivent être sécurisés, donc personne ne doit y avoir accès.

Noël PONS

Tout dépend du type de croisement ou du type d'activité que l'on peut avoir avec ce fichier. Je pense que les deux sont liés. Et à partir de là, on revient sur une utilisation qui peut d'ailleurs être contrôlée, et qui l'est effectivement.

Question de la salle

Je voulais savoir s'il y avait, encore une fois, des statistiques sur les directions ou les services qui sont plus exposés à la fraude, en entreprise ; à part les services comptables et financiers.

Comment devenir proactif dans la gestion de la fraude ?

Bernard DECOEUR

Il y a un site américain, qui s'appelle KROLL, qui donne des statistiques annuelles sur les types de fraude par secteur d'activité. Cela ne vaut pas statistique d'ensemble, mais cela donne une bonne image des tendances, des évolutions et des types de fraude.

Emmanuel PASCAL

Vous pouvez vous reporter au site de l'ACFE, au rapport qui s'appelle *Report to the Nations* et duquel j'ai extrait les statistiques tout à l'heure. Il y a des statistiques qui donnent les risques par secteur d'activité.

COMMENT UTILISER LA CARTOGRAPHIE DES RISQUES DANS LA PREVENTION ET L'ANTICIPATION DE LA FRAUDE, PAR SEBASTIEN ALLAIRE

Sébastien ALLAIRE, *Associé, Deloitte*

La première question qui se pose est : pourquoi une cartographie spécifique du risque de fraude ? Ce que l'on observe aujourd'hui dans les groupes cotés CAC 40, SBF 120, mais également non cotés, c'est une démarche de plus en plus vertueuse, gérée par le management, insufflée par les conseils d'administration ou de surveillance pour mettre en place des cartographies des risques, une cartographie globale des risques.

Au sein de ces exercices, qui peuvent présenter différentes approches – *top-down*, *bottom-up*, avec x méthodologies sur lesquelles nous travaillons –, on retrouve généralement la fraude comme un point dans la cartographie des risques présentée au management. Cela, c'est dans le meilleur des cas ; dans l'autre cas, le risque de fraude n'est pas mentionné, comme si elle n'existait pas comme un risque potentiellement majeur pour le groupe.

Lorsque l'on présente au management, ou au conseil, ou au comité d'audit, en application de la 8e directive, une cartographie des risques avec 10, 15, 20 *top risks* pour le groupe, dont un point sur la fraude, ce point fraude ne veut pas dire grand-chose, puisque la fraude est évidemment multiple, elle est polymorphe et peut se décliner dans tous les pays de manière très variée.

Notre propos est ici de dire qu'il faut aller au-delà d'un premier sondage pour savoir comment se positionnerait la fraude par rapport à d'autres risques métiers, réglementaires, stratégiques et financiers pour le groupe, et de se demander, sur la fraude, sur les différentes dimensions que constitue la fraude, comment le groupe est aujourd'hui exposé, quelle est sa vulnérabilité ? Et si cette vulnérabilité est considérée comme importante, quelles sont les actions à mettre en œuvre pour renforcer la protection contre la fraude ?

L'objectif est de cartographier les risques et non de faire une cartographie des risques ; c'est de plonger sur chaque risque de manière spécifique et non pas d'avoir une vision un peu trop *top-level* de l'ensemble de risques.

La première étape, dite vertueuse, consiste à évoquer le risque de fraude dans une entreprise et obtenir comme réponse qu'il existe un « code d'éthique ». C'est généralement la première pierre : « Nous avons réfléchi à la fraude ; nous avons défini de bonnes pratiques, les règles incontournables, déontologiques pour l'ensemble du groupe, que nous avons résumées dans un document qui peut éventuellement être traduit, qui peut d'ailleurs être ciblé sur les achats, sur la direction financière et autres, et que nous avons communiqué – ou pas – à l'ensemble de l'organisation ; et cela nous rassure, nous, management, sur le risque de fraude. » C'est vertueux, mais nous considérons que c'est assez fragile.

Une deuxième étape : on est au stade de la prévention qui s'enrichit avec une démarche un peu plus proactive ; il existe des guides, des procédures, des fiches de poste qui analysent l'aspect séparation des tâches qui est un des éléments clés de lutte contre la fraude.

La troisième étape est la détection, c'est le fameux *whistleblowing*, les systèmes d'alerte où non seulement on demande à tout le monde de bien se comporter, mais en plus, on est à l'écoute de ce qui peut arriver. Mais on en est toujours à un stade où, tant que l'on n'a pas remonté un élément d'alerte, une suspicion, on considère que tout va bien. On est donc toujours dans un mode plutôt réactif de lutte contre la fraude.

Sur le plan juridique, ce type de dispositif devrait peut-être suffire en termes de responsabilité pour les administrateurs : « J'ai défini les règles et je suis à l'écoute des possibles cas de fraude. Donc, en tant qu'administrateur, j'ai rempli mon rôle. »

Mais au-delà de la responsabilité, il subsiste l'impact que peut avoir une fraude pour une entreprise, tant au niveau financier qu'au niveau image, employés, attitude, etc. On a donc élargi l'approche vers une quatrième dimension que l'on appelle intégrée. On retrouve la prévention, et on parle de gouvernance. On retrouve la détection encore plus proactive, et on parle ici de démarche d'analyse de données, d'investigation par des outils informatiques, de *performance indicators* liés à la fraude.

Une nouvelle étape, l'anticipation, est là où l'on va situer le *Risk management*. Le discours est le suivant : dans mon entreprise, dans mon activité, selon les matières, les biens, les services que je manipule, dans les pays où je les manipule, quels seraient, de manière inhérente, de manière brute, les risques potentiels, que je vois d'ailleurs dans la presse, chez mes concurrents, et qui pourraient également affecter mon entreprise ? On se pose, au plus haut niveau, la question des risques de fraude pour ensuite sonder l'organisation sur la protection à mettre en place pour maîtriser ces risques.

Quel univers pour analyser le risque de fraude ? La réponse est évidemment : l'univers le plus large possible. Il existe différents référentiels pour déterminer ce qu'est la fraude. J'en retiens un qui donne trois grands ensembles : le détournement d'actifs, matériels ou immatériels ; la manipulation des indicateurs de performances et des états financiers (aux Etats-Unis, cette fraude comptable, c'est-à-dire l'erreur intentionnelle dans les comptes, est sévèrement punie) ; la corruption, active ou passive.

Il existe un référentiel de *Risk management*, où l'on trouve quatre grandes dimensions : la stratégie, l'opérationnel, le comptable et le financier, et la conformité réglementaire. La fraude s'applique à ces quatre dimensions. Le croisement de ces deux référentiels donnerait une vision assez globale de l'univers de la fraude.

Quelle démarche pour cartographier les risques ? Pourquoi faire du *top-down* versus du *bottom-up* ?

Le *bottom-up* est l'approche que l'on retrouve le plus fréquemment. Et aujourd'hui, ce n'est pas notre préférence. Cela se traduit généralement par un catalogue de risques, une démarche gestion des risques globale. On peut établir un catalogue de risques types sur la fraude, des schémas types de fraude que l'on communique à un certain nombre d'interlocuteurs, ce qui pose un problème évident et non négligeable de confidentialité. On communique donc ce catalogue et on demande à X opérationnels – généralement les responsables d'entités – de s'auto-évaluer, de donner leur perception de l'exposition de leur entité à tel ou tel schéma. Tout cela remonte et est agrégé et consolidé pour présenter un *top 10*, *top 15*, *top 20* au management.

Nous sommes donc assez réservés sur ces démarches *bottom-up*, à cause du processus de consolidation et d'agrégation, et nous sommes davantage pour une démarche *top-down* où l'on analysera, un par un, les sujets qui préoccupent le management.

Notre conclusion sera nuancée comme suit : nous recommandons de réaliser une démarche *top-down,* complétée par un *bottom-up* ciblé. Le *top-down* devrait être prioritaire, parce qu'il devrait permettre de cibler les risques les plus importants pour le groupe.

Comment se déclinerait, en cinq tableaux, cette démarche *top-down* ? Premièrement, l'**identification** des risques majeurs avec le management. On va essayer de capter ses préoccupations ; et l'on fera des ateliers avec le comité d'audit, l'audit interne, la DSI (la dimension informatique est essentielle), la direction générale.

Deuxièmement, on cherche à **décliner chaque risque majeur** en risques individuels et facteurs de risques par le biais d'ateliers de travail.

Troisièmement, **appréciation de l'exposition** au sein des processus concernés ou des entités concernées ; on va sonder le terrain.

Quatrièmement, **démarche sélective** de tests des schémas de fraude.

Cinquièmement, **hiérarchisation des risques résiduels**, c'est-à-dire les risques nets, une fois pris en compte les dispositifs de protection en place.

Revenons aux trois grands ensembles dont j'ai parlé précédemment : détournement d'actifs, manipulation des performances et corruption. Dans notre entreprise, le détournement d'actifs, de manière assez classique, se décline entre biens matériels et biens immatériels. Les biens matériels, dans l'exemple cité, ce seront des stocks, des immobilisations corporelles, du cash, la paie.

Je continue à analyser. Si je suis sur un détournement d'actifs - biens matériels - stocks, de quoi va-t-on parler dans mon entreprise ? On parlera de mise au rebut, de pièces et de stocks déportés, qui sont trois zones considérées par le groupe comme étant sensibles et significatives, sujettes à un risque de fraude. Et pour mes pièces, j'ai en fait deux entrepôts : j'en ai un à Angers et un à Reims. Et je suis arrivé au bout de mon analyse. Ainsi, lorsque je me pose la question de mes risques de fraude sur détournement d'actifs, parce que je considère que j'ai des stocks de pièces qui sont sensibles, qui sont à forte valeur et qui sont significatifs dans mes états financiers logés à Angers et à Reims, mon analyse devra porter spécifiquement sur mes pièces et le détournement d'actifs des pièces sur Angers et sur Reims. Voilà les deux questions que je devrai poser aux responsables de Reims et d'Angers.

Vous connaissez le fameux triangle de Cressey. Qu'est-ce qui motive la fraude ? Ou **qu'est-ce qui génère la fraude ? C'est une opportunité**. On sait comment il faut faire pour contourner le système.

C'est une motivation. Tout le monde n'est pas fraudeur ; les statistiques qui datent de quelques années ont encore été citées ce matin, sur le 20-60-20. Tout le monde n'est pas fraudeur, mais grosso modo, il y a quand même 80 % de la population qui pourrait être amenée à frauder si l'opportunité et la rationalisation le permettait.

C'est la rationalisation. C'est arriver à se dire : « Ce n'est pas grave. ».

Ces trois dimensions sont quasi systématiques sur la fraude.

Face à cela, nous proposons une approche innovante aux entreprises avec lesquelles on travaille, qui consiste à la fois à prendre les sujets par le haut et à limiter l'effort, car, vu que la fraude est polymorphe et se retrouve partout, on pourrait passer des mois et des années à analyser, dans chaque département de la société, le risque de fraude et comment s'en protéger.

Ce que nous recommandons aux entreprises avec lesquelles nous travaillons, c'est d'abord d'engager un **processus de diagnostic, d'autoévaluation**. Cette autoévaluation va partir de la perception du risque inhérent.

Nous allons par exemple nous déplacer sur le site d'Angers, et nous allons demander au responsable de ce site d'évaluer son environnement de contrôle, ces trois dimensions (motivation, opportunité et rationalisation) au sein de son entreprise. On lui demandera quel est aujourd'hui l'état des procédures, l'état de l'éthique dans son entreprise. On lui demandera comment il ressent les pressions personnelles sur les employés ; la faiblesse des indicateurs, donc la recherche d'indicateurs qui viendraient révéler des faiblesses comme l'insuffisance de suivi analytique ou de suivi de projet long terme dans ce cas concret ; le fait que l'entreprise ou l'entité ait été auditée récemment ou non ; qu'elle ait eu des suspicions de fraude récentes ou non.

Le responsable va donc juger de son environnement inhérent, de la culture locale, et des pratiques de vol qui sont communément admises et qui sont d'ailleurs rationalisées assez facilement. On lutte donc constamment contre ces pratiques. Oui, il manipule des biens que l'on peut facilement voler et qui sont à valeur marchande importante, donc sensibles, etc.

Par rapport à cet environnement, il y a un deuxième niveau d'évaluation concernant le contrôle interne sur ce site, la fiabilité des systèmes d'information et la séparation des tâches.

Chacun porte un jugement et remonte cette autoévaluation. A ceux qui remontent une autoévaluation en disant : « Je suis dans une zone à risque et je ne suis pas très à l'aise avec ce qui est en place. », le management dira : «Mets en place un plan d'action et tu as trois mois pour nous donner ta perception de l'évolution. »

Par contre, celui qui remonte un diagnostic en disant : « Je suis dans une zone à risque, mais je suis très confiant dans mes systèmes, tout va bien. Mon niveau d'exposition est très faible. », celui-là fera l'objet d'une visite des auditeurs internes ou d'une équipe ad hoc qui testera les schémas de fraude. En fonction de l'évaluation des schémas de fraude, on pourra conclure : le dispositif en place est effectivement solide et l'autoévaluation est bonne ; ou bien : non, le dispositif en place n'est pas solide, l'autoévaluation devra donc être retravaillée et un plan d'action immédiat doit être mis en place sur les points faibles identifiés.

Dans tout dispositif de gestion des risques, nous sommes dans une démarche dynamique qui progresse au fur et à mesure. Le comité d'audit devrait – comme aux Etats-Unis – être informé trimestriellement ou au moins semestriellement de cette progression. Les fraudes évoluent. Les pratiques, les techniques, les systèmes d'information évoluent.

LES ASPECTS JURIDIQUES LIES A LA FRAUDE, PAR JEAN-VICTOR PREVOST

Jean-Victor PREVOST, *Associé, TAJ*

Mon propos n'est pas aujourd'hui de traiter tous les aspects juridiques liés à la fraude, parce qu'une semaine n'y suffirait pas. Mon propos est, d'une certaine façon, de vous inciter à travailler avec votre direction juridique sur certains sujets, parce que je pense que les directions juridiques elles-mêmes ne sont pas assez impliquées sur ces sujets, et elles ne savent pas nécessairement travailler avec vous. Le juridique doit travailler avec la direction des risques, avec le contrôle interne et l'audit interne, de façon permanente.

Le contrôle interne doit travailler avec la direction juridique en amont pour détecter les fraudes ; pendant les phases d'enquête pour constituer le dossier, pour s'assurer que le dossier est solide et que l'on n'est pas en même temps en infraction sur d'autres réglementations ; et enfin, en aval, pour mesurer les conséquences juridiques. Tout le long du processus, les aspects juridiques sont très importants.

La direction juridique doit participer à la détection des fraudes. De temps en temps, notre attention peut être attirée par des contrats, ou plutôt des documents contractuels, ce qui doit nous inciter à communiquer avec la direction des risques. Le juridique a aussi un rôle à jouer dans l'établissement et le suivi des règles internes sur la fraude et sur les processus.

Il existe une grande diversité de règlements intérieurs, mais en en lisant un, on peut avoir des idées sur un certain nombre de sujets sensibles, et que l'on va gérer progressivement. Le règlement intérieur est un peu le reflet de la culture de l'entreprise.

Le dossier doit être constitué pendant les phases d'enquête. Il faut apporter la preuve de l'élément matériel de la fraude, c'est-à-dire les faits, les détournements de fonds, de marchandises, etc. Il faut apporter – c'est plus difficile, d'un point de vue juridique – la preuve de l'élément intentionnel de la fraude ; c'est-à-dire qu'il faut montrer par des écrits, par des témoignages, etc., la « connaissance » du processus par le fraudeur et sa participation au schéma ; ne serait-ce que sa connaissance du schéma est déjà un élément important. Un autre sujet très important est la problématique de preuve informatique puisque, de plus en plus, on en fait la démonstration, tout passe par l'informatique. Là, je parle de la preuve informatique, je ne parle pas des problèmes CNIL[1] que l'on évoquera tout à l'heure.

---

1 La CNIL a adopté une délibération n° 2010-369 modifiant son autorisation unique AU-004 concernant les risques de fraude et les systèmes d'alerte professionnelle (dispositifs de « whistleblowing »). La publication sur le site de la CNIL est intervenue le 8 décembre 2010.

http://www.cnil.fr/la-cnil/actu-cnil/article/article/alertes-professionnelles-la-cnil-clarifie-son-autorisation-unique-nau-004/

En pratique, toute entreprise qui souhaiterait mettre en œuvre un dispositif d'alerte professionnelle ayant un champ d'application excédant celui de l'article 1 de l'autorisation unique AU-004 modifiée, doit OBLIGATOIREMENT suivre la procédure d'autorisation individuelle de la CNIL (avec un minimum deux mois pour obtenir une telle autorisation).

Pour les entreprises qui ont déjà mis en place un système d'alertes professionnelles, il n'est pas nécessaire de procéder à un nouvel engagement de conformité à l'autorisation unique AU-004 modifiée dès lors que le périmètre du dispositif d'alerte professionnelle respecte le nouveau champ défini par la CNIL.

En revanche, en ce qui concerne les entreprises dont le dispositif d'alerte professionnelle a fait l'objet d'un engagement de conformité à l'autorisation unique AU-004 initiale mais dont le champ va au-delà de celui défini à l'article 1 de l'autorisation unique AU-004 modifiée, elles devront, au choix et dans un délai de 6 mois à compter du 8 décembre 2010, soit d'ici le 7 juin 2011 :

La légalité des procédures pendant la phase d'enquête est primordiale. S'il y a des problèmes de légalité, d'infraction, aussi bien sur le droit du travail que sur le droit des données personnelles, je pense que l'enquête peut être remise en question. L'objet de la fraude n'est pas particulièrement de poursuivre l'individu fraudeur, mais plutôt de gérer les dommages qui en découlent.

Du point de vue du droit des salariés, je reviens à ce qui a été dit tout à l'heure, vous regarderez la pression personnelle, le train de vie, etc. Mais vous ne pouvez pas non plus être intrusif vis-à-vis de la vie privée de vos salariés. Il y a donc un équilibre à trouver. C'est un peu la même chose que du point de vue CNIL. Le grand principe de la CNIL est que l'intrusion doit être minimale par rapport à l'intérêt de l'entreprise ; il ne faut pas aller chercher les informations tous azimuts.

Mesurer les conséquences juridiques de la fraude pour le fraudeur. Cela fait aussi partie d'une analyse juridique. Il peut y avoir une action pénale. Le problème d'une telle action est que ce n'est pas vous qui la contrôlez, mais le ministère public, et ce n'est pas forcément la façon la plus rapide et la plus efficace d'obtenir une compensation, dans la mesure où vous essayerez d'obtenir une compensation du fraudeur (ce qui n'est pas l'essentiel de ce que l'on recherche quand on résout un problème de fraude).

Mesurer les conséquences juridiques de la fraude pour l'entreprise. Un certain nombre de fraudes sont faites soi-disant dans l'intérêt de l'entreprise. Il y a de grands domaines d'activité dans lesquels, en France, ces sujets sont classiques : les marchés publics, le droit de la concurrence… La difficulté est que l'on ne peut pas exercer une surveillance de tous les moments. Il faut donc intégrer ces sujets dans la culture de l'entreprise, via les règlements intérieurs, etc. Il faut en parler et les mettre sur la table.

QUESTIONS/REPONSES

Question de la salle

Que recommandez-vous pour sécuriser un entretien avec quelqu'un à l'égard de qui on a des soupçons de fraude, en ce qui concerne la prise de notes en cours d'entretien ? Est-ce que ce genre de minutes a une valeur, ensuite, dans un dossier que l'on adressera au ministère public ?

Jean-Victor PREVOST

Non, cela a une valeur assez limitée. Cela permet simplement de reconstruire ensuite l'histoire. De toute façon, le ministère public fera sa propre enquête.

Question de la salle

Vous parliez tout à l'heure d'intrusion. J'ai l'occasion d'auditer des agences et je dois regarder dans les ordinateurs qui appartiennent à la société. Et pourtant, il y a des dossiers privés ou personnels.

(i) soit déposer une demande d'autorisation individuelle auprès de la CNIL, étant désormais entendu que les dispositifs non conformes à l'AU-004 modifiée, sont ceux qui couvrent notamment les domaines de la propriété intellectuelle ou de la discrimination, et qui doivent par conséquent faire l'objet d'une demande d'autorisation individuelle

(ii) soit modifier le champ de leur dispositif de tel sorte qu'il soit conforme à l'article 1 de l'autorisation unique AU-004 modifiée auquel cas aucune formalité ne devra être accomplie auprès de la CNIL (sous réserve du contrôle possible de la CNIL à compter du 8 juin 2011).

Comment devenir proactif dans la gestion de la fraude ?

Jean-Victor PREVOST

Le problème est que l'usage privé des moyens informatiques mis à disposition des salariés est toléré. Toutefois, cette tolérance ne permet pas à l'entreprise d'aller dans l'espace privé, que l'on appelle l'espace personnel virtuel du salarié.

Question de la salle

J'ai déjà trouvé des faux dans ce genre de dossier. Est-ce que j'ai ou pas le droit de le signaler en annexe d'un rapport ? Sans doute, non.

Jean-Victor PREVOST

Si vous êtes en mesure d'établir que vous l'avez fait sans violer les droits du salarié, oui. Mais c'est vrai que l'on va vous demander comment vous avez récupéré cette information. C'est délicat. Après, c'est une question de faits.

Remarque de la salle

Juste pour apporter un complément de réponse à la question qui vient d'être posée. En matière de recherche informatique, il est interdit d'aller voir dans les dossiers intitulés « personnel ». Pour le reste des dossiers, le poste informatique est présumé appartenir à l'employeur. Et donc, en France en tout cas – ce n'est pas partout comme cela –, il n'y a aucun problème pour aller voir à l'intérieur.

Jean-Victor PREVOST

Oui, c'est juste. Il faut effectivement que le dossier soit identifié comme étant personnel.

Romain MARIE

Combien de temps faut-il prévoir pour établir une cartographie des risques de fraude, dans une entreprise de taille moyenne ?

Ce sont des interventions en général assez lourdes, sur plusieurs semaines. Que préconisez-vous comme type d'intervention ?

Sébastien ALLAIRE

Cette démarche est généralement entreprise suite à une décision, du management ou du conseil, et, au maximum, elle devra être réalisée dans l'année qui suit. C'est la phase maximale. Et quand je dis « une année », cela prend en compte un travail important en interne, de définition de démarche, de communication, d'analyse, éventuellement d'implication d'experts, et de synthèse, de validation, de *reporting* au management.

Les bonnes pratiques se positionnent plutôt sur une échéance de six mois. Il vaut mieux faire peu et faire bien que de vouloir aller trop vite. Donc, commencer – surtout si la démarche est un peu innovante – par mener ce que l'on appelle des pilotes, c'est-à-dire une ou deux analyses, sur un pays et sur un type de fraude, de manière transverse, par informatique, et être capable, sur deux analyses, de faire un rapport dans les six mois qui viennent.

Romain MARIE

Comment devenir proactif dans la gestion de la fraude ?

J'ai une question sur l'assurance liée à la fraude. Que recommandez-vous en particulier ? Je pense qu'il faut être assez vigilant sur l'assurance de la fraude. Les sociétés peuvent se prémunir. Il y a parfois des clauses très importantes à surveiller, par exemple la date du dernier passage de l'audit interne dans votre politique d'assurance fraude. Si vous n'avez pas surveillé cette clause, cela peut vous réserver des surprises et rendre ineffective votre politique d'assurance, au cas où vous auriez souscrit une politique d'assurance fraude.

Sébastien ALLAIRE

Je n'ai pas d'élément de réponse très concret. Quand on est face à un risque, on analyse le risque de survenance. Ensuite, le management ou la direction des assurances ou opérationnelle peut expliquer que même si le risque se concrétise, on est couvert. Mais on est généralement couvert sur les aspects financiers, ce qui n'empêche qu'il peut y avoir une responsabilité juridique engagée, il peut y avoir un impact image engagé, il peut y avoir une relation partenaire ou client détériorée.

Ce sera donc pris dans l'analyse des aspects de recouvrabilité des pertes financières, mais ce que l'on recherche dans l'analyse du risque de fraude, ce sont les moyens de limiter la survenance.

COMMENT REAGIR FACE A UN SOUPÇON DE FRAUDE OU TRAITER D'UN CAS AVERE ?

Jean-François SAUTIN, *Président de l'Unité de Recherche, Senior vice-President Group Audit, Lafarge*

Emmanuel PASCAL, *Audit Manager, Brakes Group*

Jean-François SAUTIN

Que fait-on quand, en dépit de toutes les précautions prises, de tous les programmes de prévention, etc., on se trouve confronté à une situation de soupçon ou, ce qui est plus rare, à un cas avéré.

Nous allons nous placer dans une démarche de synthèse et de pratique opérationnelle, si je puis dire, en re-balayant les principaux aspects de cette gestion de crise, car il s'agit bien de cela. Comme toujours, dans de ce qui va être dit, il n'y a pas de recette magique, il y a des points de repère. Tous les points de repère qui ont été donnés depuis ce matin sont pertinents. Et évidemment, cela va sans dire, à chaque étape, il y a un jugement managérial qui doit être porté. Ce jugement managérial, comme toute situation de management, veut dire que l'on est assez seul. Et le point de rappel est que vous serez seul quand cela vous arrivera, parce qu'on est toujours seul face à cette problématique de gestion d'une crise.

On va parler de préparation, d'anticipation ; on va parler de calibrage des moyens, de gestion, de clôture, et de capitalisation.

Emmanuel PASCAL

Quels sont **les risques liés à une investigation** ? Le risque principal, lorsque l'on fait une investigation – sur un soupçon ou un cas avéré – est de **ne pas trouver**. «Ne pas trouver », cela veut dire ne pas trouver la fraude, ne pas pouvoir la prouver, ne pas avoir de suspect et ne pas avoir d'élément. A ce stade, on ne peut pas résoudre le problème. C'est une éventualité qu'il ne faut pas rejeter. Quand on mène une investigation, on peut effectivement n'arriver à rien.

Trouver sans preuve. On a compris la fraude, on a trouvé les éléments. Mais, comme vous le savez, il y a généralement un ou des suspects. Il faut pouvoir mener à bien une procédure judiciaire, éventuellement ; et sans preuve, on ne pourra rien faire pour ce qui est de la sanction ou de la procédure judiciaire.

Dans une investigation, on peut **accuser des innocents**. C'est pour cette raison que l'on doit être extrêmement prudent et respecter les règles de confidentialité.

Ne pas respecter la législation. Il y a deux législations très importantes, d'une part celle qui est liée aux RH, aux Prud'hommes ; d'autre part celle de la CNIL : enfreindre ses lois fait courir un très gros risque à l'entreprise.

Réagir trop tard. Certes, il ne faut pas réagir trop vite, mais si l'on attend trop, la fraude peut continuer. Et vous n'êtes pas sûr de récupérer votre argent.

Réagir trop tôt. Cela rejoint un peu le point « trouver sans preuve ». Si vous prenez une personne et que vous la licenciez aussitôt, vous coupez tout, et si la personne a fait d'autres fraudes, vous n'avez qu'un morceau du puzzle.

La mise en danger des équipes. Il existe des zones sensibles, il faut donc arriver à sécuriser ses équipes qui peuvent être mises en danger.

Perdre son temps et gaspiller des ressources. Vous comprendrez que si l'on fait appel à des intervenants extérieurs, et que votre soupçon de fraude n'est pas vraiment fondé, c'est une perte de temps et d'argent.

Jean-François SAUTIN

Comment gérer une fraude, gérer une crise ? Il faut prendre le temps, ne pas aller trop vite, bien raisonner ce que l'on fait.

Je reviens sur l'idée que l'on est dans un cadre d'incident industriel dont il faut d'abord prendre la mesure, comprendre ce à quoi on est confronté et, très vite, raisonner sur les conséquences en interne et en externe.

Vous n'êtes pas obligé de travailler seul. Très vite, constituer une équipe, sur la base de personnes qui doivent savoir. On limite, pour des questions de confidentialité, mais on engage des compétences, qu'elles soient légales, RH, sécurité, sûreté, éventuellement communication, etc., pour créer une première cellule qui va mesurer les conséquences de la situation telle qu'on la perçoit, car c'est très souvent plus une perception qu'une réalité. Il y a les problèmes d'image, il y a le moral des troupes, il y a des actionnaires, il y a la réputation. Et la gestion des personnes fragiles.

Les **enjeux**. Il y a des enjeux légaux et des enjeux de ressources humaines. Il faut, peut-être pas d'entrée de jeu mais assez vite, commencer à raisonner sur le type de sanction : va-t-on aller vers une enquête de police et une action en justice ? Va-t-on traiter cela plutôt en interne, avec tout l'arsenal ? Tout cela, ce sont des questions de jugement qui appartiennent au management. Et il faut là encore que la sanction soit proportionnée à la situation telle qu'elle aura été analysée.

Le **processus** est rigoureux. Il est vrai que les auditeurs sont a priori assez bien câblés pour faire une grande partie de ce travail-là, mais je crois que la chose la plus importante est la compétence et l'expérience. C'est une question de jugement, là encore, et il faudra être très attentif à la compétence et à l'expérience des personnes qui seront impliquées dans cette cellule de crise, être convaincu qu'elles ont le recul et l'expérience nécessaires pour gérer l'affaire avec bon sens, avec une bonne compréhension de toutes les dimensions du problème.

Emmanuel PASCAL

Il faut se préparer à bien gérer une crise, à identifier, à tester.

Parmi **les intervenants internes** il y a les RH, la direction juridique, mais aussi la sécurité, et surtout l'informatique.

Les intervenants externes, c'est-à-dire les prestataires. On est là dans une démarche classique : on identifie, on teste, on rencontre, on fait des devis, on demande aux gens comment ils travaillent. Il vaut mieux le faire avant que dans le feu de l'action. Il ne faut pas négliger les intervenants externes, surtout dans les environnements que l'on connaît peu ou pas.

Les autorités. Il faut se préparer aux rencontres avec la police, la gendarmerie, la justice. Quand vous passez trois heures en interrogatoire à la police, il faut être prêt. On va vous poser des questions. Vous avez peut-être réussi votre investigation de votre côté, mais il faut que vous réussissiez l'autre étape qui est la procédure judiciaire. Cela se prépare. Il est bon de se faire conseiller par la direction juridique au préalable.

Les assurances conseils : vous allez contacter vos agents d'assurance. Il faut relire vos polices et savoir comment vous allez travailler avec eux.

Vous avez donc compris qu'il faut organiser a priori et établir un processus de décision : comment va-t-on passer d'une étape à l'autre ? Va-t-on continuer ? Comment va-t-on décider que l'on va prendre

des intervenants extérieurs ? Qui va décider du budget ? A-t-on un budget ? Qui va faire quoi (mise à disposition de moyens) ?

Dans le même temps, c'est aussi l'étude de tous les cas antérieurs, qui vous permettront d'éclairer votre travail. Il faut savoir anticiper.

Jean-François SAUTIN

Sur le calibrage des moyens, je vais aller très vite, parce qu'on a déjà tout dit.

Il faut savoir où se positionner dans la hiérarchie. C'est un point important, au départ d'une affaire. Quand les choses ne sont pas très claires, il vaut mieux comprendre qui peut être impliqué.

Quelquefois, le N+1 d'une personne soupçonnée est impliqué, et on ira donc plutôt travailler avec le N+2, voire le N+3 pour lancer les opérations. Là encore, il n'y a pas de recette, on joue un peu le résultat de l'enquête, parce qu'on peut toujours se tromper. Mais il faut anticiper et n'impliquer les gens que vraiment à bon escient, pour ne pas faire déraper un processus d'enquête.

Emmanuel PASCAL

Gérer la crise, c'est maîtriser les étapes. Il y a différentes étapes qui impliquent des prises de décision. Vous devrez documenter le processus d'enquête. Dans ce cas-là, vous n'êtes plus des auditeurs internes, vous faites partie d'une équipe qui peut être contrôlée. Il faut donc bien avoir en tête que c'est un rôle un peu différent et qu'un jour, on peut vous demander des comptes. Vous êtes dans un processus qui est auditable.

Il faut ensuite que vous rentriez dans le moule du processus judiciaire. Tout ce qui est preuve récoltée doit donc être conforme à ce que l'on attend en termes de preuves.

Je le répète, il faut déléguer à bon escient. Si vous garantissez la confidentialité et que vous comprenez que vous n'êtes pas capable de mener cela tout seul, il faut arriver à déléguer. C'est pour cela qu'il faut s'être bien coordonné avec les intervenants extérieurs, avoir de bonnes relations avec eux, et avoir mis au point au départ un processus de relation et de décision.

Avec la justice et la police, il faut également bien se coordonner.

Jean-François SAUTIN

Puis vient le temps de conclure. Comme dans toute gestion de crise, il faut d'abord gérer le cas. Si la malversation est avérée, vous devez décider si vous intentez une action en justice, considérer les aspects de communication, etc.

Il faut aussi accepter la possibilité d'un échec. On ne trouve pas toujours. Ce sont certainement les cas les plus frustrants, parce qu'on a un arrière-goût, une amertume de ne pas avoir clarifié complètement la situation, mais il est important de pouvoir mettre un point final, éviter l'acharnement, éviter un mauvais suspect simplement parce que vous voulez absolument conclure et faire un exemple.

Par contre, quelle que soit la situation que vous avez analysée, c'est un point de vigilance. Il y a toujours une capitalisation à faire, même si vous n'avez pas réussi à conclure ce cas-là.

Mais il faut surtout arriver à tourner la page. Il est important pour les équipes de pouvoir dire : « On a cherché, on n'a rien trouvé. C'est fini. » Jusqu'à ce qu'il y ait une autre preuve ou un autre indice.

Emmanuel PASCAL

Comment devenir proactif dans la gestion de la fraude ?

Le dernier point est **la capitalisation**. C'est l'analyse critique de la crise, une sorte de débriefing. Il est de bonne pratique, après une investigation, de voir ce qui s'est passé, en termes de délai, de moyens ; a-t-on bien travaillé sur la qualité de preuve ? La crise a-t-elle été bien gérée ?

Ne pas oublier de documenter la base des cas de fraude. Il y a une législation à respecter pour cela.

Jean-François SAUTIN

Quelques questions nous ont été posées.

Existe-t-il des dispositifs à mettre en place pour protéger les auditeurs internes face aux conséquences extrêmes qui pourraient être liées à leurs activités de détection de fraude ? Exemple : suicide du fraudeur.

C'est une question brutale. Je pense qu'il faut être très modeste quant à la réponse qu'il faut apporter à cette question.

Je reviens sur la notion de jugement. Il n'y a pas de réponse absolue à cela. Il est évident que, plus vous aurez su vous entourer des bons conseils pour lancer l'investigation, mieux vous protégerez vos auditeurs sur ces choses-là.

J'ai en tête un cas récent d'une enquête qui a été menée dans un pays que je ne citerai pas, dans un temps que je ne citerai pas. Il est évident que les contrôleurs internes impliqués, pour parler très simplement, avaient peur. Cette peur-là n'est pas saine et il ne faut pas exposer les gens à des situations dans lesquelles ils ont peur. Ils avaient peur des conséquences peut-être de type mafieux ou de menaces comme cela.

Dans ce cas il ne faut pas hésiter et vouloir économiser trois sous, alors qu'il y a des gens dont c'est le métier, des gens qui ont généralement un parcours professionnel qui les a exposés à ce type d'enquête et qui savent comment se comporter, et qui ont les réflexes de sûreté qu'il faut.

Concernant le cas d'une personne fragile, là encore, je n'ai pas de réponse. Je crois qu'il faut être extrêmement prudent et, s'il y a le moindre soupçon de fragilité, travailler avec des conseils extérieurs et éviter de déclencher une crise qui amènerait au suicide, bien évidemment.

Emmanuel PASCAL

Je n'ai rien à ajouter.

Question : Que recommandez-vous en termes de remontée d'information auprès de la direction générale ? Forme, fréquence, à partir de quand la tenir informée ?

Jean-François SAUTIN

Je crois qu'on est vraiment là dans la culture de l'entreprise. Je sais que dans mon groupe, je suis invité à chacune des réunions du comité d'audit et, ex-fonction, je fais ce que l'on appelle un point fraude, parce que nous avons une politique de remontée des cas de fraude qui demande à tous les patrons d'entité de partager avec la tête de groupe, c'est-à-dire moi-même et le responsable du département juridique, tous les cas dont ils ont connaissance, sans seuil de matérialité.

Ce qui fait d'ailleurs couler beaucoup d'encre, parce que les patrons de l'entité ne comprennent pas toujours très bien pourquoi, lorsqu'on leur a volé trois sacs de ciment quelque part, il est important que Paris soit informé. On essaie, à l'inverse, d'être très raisonnable et, lorsque les gens jouent bien le jeu et nous informent, on ne leur met pas de pression pour trois sacs de ciment.

Comment devenir proactif dans la gestion de la fraude ?

L'idée de remonter les cas de fraude permet de prendre la température de l'organisation. Et je crois qu'il est important, pour pouvoir analyser les cas, de sentir comment cela se passe dans la réalité des opérations. C'est pourquoi j'ai l'opportunité, deux ou trois fois par an, de faire un point avec le comité exécutif du groupe pour parler du suivi de la fraude, des cas détectés, etc.

Emmanuel PASCAL

Question : Y a-t-il un risque à mentionner un nom dans un rapport d'audit (à la différence de l'inspection générale) ? Si oui, lequel ?

Vous êtes en cours d'investigation ; imaginez que vous mettiez un nom dans le rapport d'audit et, en fait, ce n'est pas la personne. Vous allez laisser un nom dans un document. Quand on va conclure, si ce n'est pas la bonne personne, il faut que l'on ne puisse plus revenir sur cette personne-là. Le risque est donc là : à un moment, on a marqué que M. Untel était suspect dans une affaire.

Si j'ai bien compris, « à la différence de l'inspection générale », je crois, pour être passé dans le public, qu'on ne met pas les noms dans les rapports. Je suis tout à fait d'accord avec le fait de ne pas mentionner les noms dans les rapports d'audit, mais plutôt les fonctions.

Jean-François SAUTIN

Notre pratique est la suivante : lorsqu'une mission d'audit est confrontée à une situation qui fait penser qu'il y a une fraude ou une suspicion de fraude, d'une part le directeur de mission est immédiatement informé ; je suis également immédiatement informé de la situation et nous en discutons avec l'équipe d'auditeurs. La règle générale est de traiter ce cas en dehors du rapport d'audit.

On reste donc concentré sur l'évaluation des processus et on alerte le management, par lettre séparée qui, là encore, ne contient pas de nom de personne, etc., mais qui décrit bien des situations et qui peut éventuellement ensuite, en comité restreint, déclencher une investigation.

Emmanuel PASCAL

Question : existe-t-il un document synthétique pour les bonnes pratiques en matière de prévention de fraude ?

On a cité beaucoup d'ouvrages. Il y a beaucoup de référentiels. Il y a aussi un document de l'IIA et de l'IFACI sur la fraude qui est sorti cette année, et qui a été traduit en français.

Jean-François SAUTIN

Il y a un point que je veux mentionner là, qui a été dit dans le courant de la journée, mais que je veux rappeler, parce que pour moi, il est très important : la première prévention de la fraude est la maîtrise de votre métier, la connaissance du métier : sensibilité aux signaux faibles, sensibilité aux petits dysfonctionnements.

Je pense à un cas assez banal, une toute petite fraude qui consiste, lorsque l'on charge une barge avec des sacs de ciment, à s'assurer qu'il y a beaucoup de sacs qui crèvent, parce que quand un sac de ciment crève, le ciment se répand, on le reprend à la pelle, on le remet dans un sac à part. Et dans certains pays, cela se vend très bien au marché noir. Ce sont des choses comme cela, les connaissances du métier. Un contremaître ou un directeur de station qui est sensible au fait que le taux de casse «normal » des sacs est de l'ordre de 0, 5 %, et qui tout d'un coup se dit : « Tiens, il y a

2 %. Qu'est-ce qui se passe ? », met le doigt sur le premier point d'entrée de la détection de la fraude.

Emmanuel PASCAL

Question : en matière de fraude, il y a ceux qui cherchent, ceux qui trouvent… il y a la part de raisonnement malhonnête…

Ce que j'ai dit, c'est qu'il fallait se mettre à la place… il faut avoir un peu d'imagination. C'est vrai que ce n'est pas toujours facile.

Je rappelle quand même qu'il y a énormément de classiques. 90% des fraudes sont classiques. Mais il faut savoir sortir des sentiers battus.

Question : quel est le rôle des RH ?

Le rôle des RH est de prévoir les sanctions. C'est aussi un rôle de conseil : il y a ce que l'on peut faire et ce qu'il ne faut pas faire. Dans le cadre d'une investigation, l'audit doit beaucoup collaborer et avec les RH et avec le juridique.

Jean-François SAUTIN

Je crois que l'ensemble de ces acteurs est impliqué. Je pense que, ex-fonction, les auditeurs internes et les contrôleurs internes seront plus facilement des catalyseurs parce qu'ils sont plus proches de situations qui peuvent amener à des cas de fraude, et ils doivent donc être armés pour aborder ces sujets-là. Mais, très vite, le sujet dépasse le strict cadre de l'audit interne ou du contrôle interne.

Ce que j'essayais de dire ce matin, en introduction, c'était que c'est un problème de l'organisation dans son ensemble. Il faudra donc très vite mobiliser soit différentes fonctions, soit des opérationnels, et chaque cas sera un cas particulier.

QUESTIONS/REPONSES

Question de la salle

Vous avez abordé un peu le problème tout au long de la journée, mais je trouve que vous n'avez pas suffisamment mis en évidence le rôle de manager d'une équipe. Je suis au contrôle interne, et on dit souvent que le management, c'est le contrôle de premier niveau, de deuxième niveau par rapport aux opérations liées à l'activité.

Il peut y avoir des failles, des dysfonctionnements de sécurité dans le processus qui se déroule sous la responsabilité du manager, et ce dernier peut être amené à avoir sinon des soupçons tout au moins des craintes. Il est donc éventuellement conduit à mettre en œuvre les premières actions de couverture de ces failles de sécurité, s'il en a la possibilité, ou bien à alerter sa hiérarchie.

J'ai trouvé que le manager n'était pas forcément systématiquement repositionné avec l'auditeur.

Jean-François SAUTIN

J'appuie tout à fait votre propos. On n'en a peut-être effectivement pas assez parlé, mais peut-être cela reflète-t-il le fait que, dans beaucoup d'organisations, on a aujourd'hui un peu de mal à trouver le ton juste, ou à s'impliquer de façon constructive et détendue dans cette problématique.

Comment devenir proactif dans la gestion de la fraude ?

Emmanuel PASCAL

Je répète ce que j'ai dit ce matin, la détection ne se fait pas toute seule. Les managers sont en première ligne. Ce sont eux qui vont voir leur responsable s'ils sentent qu'il y a quelque chose qui ne va pas, c'est vers eux que leur N-1 ou N-2 vont se tourner.

Et, comme je l'ai expliqué ce matin, la voie hiérarchique est une voie normale pour la remontée des fraudes. Le rôle du manager doit être valorisé. Le manager doit être responsabilisé car il est au cœur du système.

Romain MARIE

Puisque l'on parle de manager, j'ai un exemple concret. Dans un pays de l'Est, une fraude majeure a été commise. Le manager a été complètement court-circuité par le fraudeur qui avait créé un espace de non-contrôle. Cela s'est évidemment retourné contre le manager qui n'était pas basé dans le même pays, et sur lequel cette fraude avait jeté un discrédit total concernant ses capacités managériales.

Jean-François SAUTIN

Chez nous, grâce à Sarbanes-Oxley, on a mis en place un processus de certification et de remontée de lettres de certification qui permet à chaque patron d'entité de signer formellement une lettre dans laquelle il déclare n'avoir connaissance que de certains cas de fraude ou de l'absence de cas de fraude.

Question de la salle

Dans l'entreprise où je travaille, on fait la distinction entre la fraude interne et la fraude externe. Est-ce que vous faites aussi cette distinction, ou parle-t-on uniquement de fraude interne, aujourd'hui ?

Emmanuel PASCAL

Tout ce que l'on vous a dit aujourd'hui concerne la fraude externe et interne. Lorsqu'il y a collusion entre un employé et un fournisseur, c'est quoi ? C'est de la fraude externe ou de la fraude interne ? C'est les deux. Je ne pense pas que l'on puisse les distinguer.

TABLE RONDE : QUELLE EST L'INCIDENCE DU SECTEUR D'ACTIVITE SUR LE DISPOSITIF DE LUTTE CONTRE LA FRAUDE ?

ANIME PAR **ROMAIN MARIE**, *Senior Vice-president Internal audit & Internal control, Alstom*

AVEC **VALERIE BERCHE**, DIRECTRICE AUDIT GROUPE, FRANÇAISE DES JEUX

MARC FOURRIER, DIRECTEUR DE LA CONFORMITE, ALLIANZ

MICHEL LAPORTE-MARROUX, INTERNATIONAL FRAUD & REVENUE ASSURANCE MANAGER, FRANCE TELECOM ORANGE

CATHERINE VAN DER LINDEN, DIRECTEUR SECTORIEL AUDIT GROUPE, COORDINATEUR RISQUES DE FRAUDE CORPORATE, TOTAL

Romain MARIE

Je vous propose **quatre thèmes** dont nous allons débattre. Le premier est lié aux **types de risques de fraude** auxquels votre entreprise est confrontée. Quelle organisation a-t-elle été mise en place dans votre structure pour lutter contre ces risques ?

Le deuxième thème traitera des **dispositifs de lutte contre la fraude** que vous avez mis en œuvre pour être proactifs.

Le troisième thème portera sur les **exemples de fraudes** auxquelles vous avez été récemment confrontés.

Le quatrième thème sera : comment avez-vous réussi à **impliquer les managers** de votre entreprise dans la lutte contre la fraude ?

Catherine VAN DER LINDEN, à quel type de risque de fraude votre entreprise est-elle confrontée ? Quelle organisation a-t-elle été mise en place dans votre structure ?

Catherine VAN DER LINDEN

Dans le secteur industriel, on est en général confronté à une très large diversité de risques de fraude, de source interne et de source externe, et de cas de collusion entre les deux. La rupture interne/externe est assez peu pertinente, je pense, dans ces secteurs.

Les cas que l'on est le plus souvent amené à traiter sont les risques de vols sur les produits, et sur toute la chaîne, aussi bien matières premières et produits finis, que moyens de production, ou pièces de rechange, ou outillages. Selon nos industries, on est amené à traiter parfois avec des outillages qui peuvent avoir une valeur commerciale, et qui peuvent donc aussi faire l'objet de détournements d'actifs. C'est bien sûr un gros enjeu dans le secteur industriel qui est le nôtre.

L'autre cas, ce sont les détournements d'actifs financiers : cash, chèques, virements électroniques, falsification de factures, détournement dans les paiements versés aux collaborateurs. La palette est assez vaste.

Le troisième cas est ce que je pourrais appeler les démarches non éthiques dans la conduite des affaires : les problématiques de corruption, les problématiques d'entente, l'utilisation de situations personnelles, donc de conflits d'intérêt au détriment de l'entreprise. Ce sont des enjeux qui peuvent être importants dans les processus d'achat ou commerciaux des entreprises.

Le dernier cas concerne la manipulation, la falsification de données opérationnelles ou financières.

Cette diversité conduit en pratique à impliquer et à coordonner l'action de très nombreuses fonctions dans le dispositif de lutte contre la fraude. Cela veut dire qu'il faut aussi bien travailler avec des logisticiens que des acheteurs, des financiers que des informaticiens, des opérationnels des différents processus, mais aussi des spécialistes qui vont appuyer la démarche de prévention ou de détection, par exemple dans les domaines de sûreté, juridiques. Les contrôleurs internes ou auditeurs internes sont bien sûr partie prenante.

C'est donc un mélange de coordination et d'animation impliquant à la fois les opérationnels, de manière très étroite, et des spécialistes de l'animation du dispositif de prévention de la fraude.

Cela conduit aussi, du fait de la diversité de ces typologies, à mettre un accent très fort sur les actions de sensibilisation et de formation, à la fois globales sur l'ensemble d'une organisation, d'une filiale, et parfois très ciblées par métier pour faire prendre conscience aux opérationnels de la typologie de fraude spécifique à leur métier.

Romain MARIE

M. LAPORTE-MARROUX, quelles sont les particularités concernant le secteur télécoms ? Quelque peu différentes, j'imagine.

Michel LAPORTE-MARROUX

Pour le secteur des télécoms, nous avons à gérer, dans l'équipe *Fraud & Revenue assurance*, toutes les fraudes quelles qu'elles soient, internes ou externes, au bénéfice du fraudeur lui-même ou de l'entreprise, ou Telco ou non-Telco (non-Telco, c'est le cycle achats, comptabilité, trésorerie, etc.).

En matière de fraude purement télécommunications, nous avons affaire à trois grandes familles. Pour simplifier les choses, il y a la fraude qui s'attaque à nos clients ; il y a l'attaque par des virus informatiques; il y a les fraudes attachées aux nouveaux services que nous proposons dans certains pays, surtout les pays en voie de développement, ce que nous appelons le *mobile banking*. C'est très similaire au produit Monéo que nous avons sur notre carte bleue, un système de portefeuille électronique attaché à la petite puce de votre carte bleue. Nous proposons maintenant ce même type de service dans la puce qui est dans votre téléphone mobile. Nous transportons et stockons de la monnaie pour le compte de nos clients. C'est une activité bancaire. Vous imaginez la tentation, pour les fraudeurs, d'accéder à ces fonds, de les détourner. Sachant qu'il y a également la possibilité, dans certains pays, de faire des transferts de fonds à l'international, on tombe potentiellement dans le blanchiment d'argent.

On a souvent affaire à des fraudeurs qui cherchent à obtenir des services ou des produits gratuitement, à notre détriment en tant qu'opérateur télécom, dans le but de les revendre sur des marchés parallèles. Les mobiles sont des objets facilement transportables et très liquides, puisqu'ils sont facilement revendables, ne serait-ce que sur e-Bay. Ce sont des mobiles que nous subventionnons. Le prix que vous voyez en magasin, pour citer un iPhone, est peut-être autour de 100 euros ; sur le marché, vous pouvez le revendre 600 euros. Beaucoup de gens exploitent cette possibilité pour financer leurs propres activités ou générer de la trésorerie.

Quelque chose de plus commun et de plus important est l'attaque de nos réseaux ou l'exploitation de faiblesses du réseau pour acheminer des communications, des appels. Cela permet à d'autres opérateurs, qui ne sont pas forcément très honnêtes, de bénéficier de tarifs exceptionnels, peut-être pour joindre certains pays ou certains opérateurs.

Pour répondre à ce type de fraude, nous avons mis en place une assez grosse structure de 26 personnes en centrale multiculturelle – 5 nationalités réparties sur 4 pays en Europe – et multidisciplinaire – il y a des financiers, des experts techniques, des experts réseaux, systèmes

d'information, et également des spécialistes métier de notre activité télécom, en termes de marketing, de gestion client, de facturation.

Romain MARIE

M. FOURRIER, vous, dans l'assurance, êtes dans une activité dématérialisée. Quelles sont vos problématiques ?

Marc FOURRIER

Dans le secteur de l'assurance, on a souvent tendance à parler de fraude interne et de fraude externe, même s'il y a évidemment toujours le recoupement de la collusion.

La **fraude interne**, c'est tout ce qui est commis à l'intérieur de l'entreprise, soit par des salariés, soit par des mandataires.

La **fraude externe**, ce sont des tiers qui déclarent des faux sinistres ou des sinistres exagérés, avec de fausses assurances en main.

Sur la fraude interne, on est surtout sur des problématiques – notamment au travers des réseaux de distribution – de détournement de primes. Là, on touche les clients, et c'est donc particulièrement sensible pour nous. En termes de risque, il y a non seulement le risque financier, mais aussi le risque d'image.

On trouve aussi en gestion, les problématiques de fraude informatique, de détournement de fonds, de manipulation comptable, de faux sinistres.

Concernant le traitement, nous avons deux approches. Sur la fraude interne, on a en général une volumétrie assez faible, pour des montants qui peuvent être relativement importants. C'est du cas par cas, alors que sur l'activité fraude, et notamment fraude externe, fraude à l'assurance, on est sur une approche « industrielle ». Industrielle, pourquoi ? Parce que, sur les 6 millions de clients et les X millions de sinistres qui arrivent par an, il y a un nombre très élevé de fraudes externes. Des études montrent que cela peut représenter entre 3 et 6 % des primes collectées, donc du chiffre d'affaires. Et ce sont des dizaines de milliers de cas par an.

On est donc obligé d'avoir une approche sur la fraude externe complètement intégrée dans les processus de gestion, dans les centres de gestion ; avec, de plus en plus, l'utilisation d'outils informatiques de profilage ou de recherche de schémas récurrents.

Avec la fraude interne, on est sur une cellule centrale. Il y a un dispositif antifraude interne, prévention, détection, traitement, qui est situé en centrale, à la direction de la conformité, avec une politique bien construite.

En termes d'impacts, ceux-ci touchent à la réputation dans la fraude interne, avec des impacts techniques sur la rentabilité des produits. Nous devons donc être plus efficaces dans la lutte contre cette fraude.

En termes de confidentialité, autant sur la fraude interne, on n'échange pas, autant, sur la fraude externe, d'un point de vue technique, en risques opérationnels partageables, on se concerte entre spécialistes du domaine.

On a donc tendance à séparer fraude interne et fraude externe, même si le sujet reste évidemment la fraude dans son ensemble.

Romain MARIE

Comment devenir proactif dans la gestion de la fraude ?

A la Française des jeux, à quelles problématiques êtes-vous confrontés, et comment y répondez-vous ?

Valérie BERCHE

Pour réaliser les 10 milliards de chiffre d'affaires que la Française des jeux réalise annuellement, nous ne sommes « que » 950 personnes, mais dotées d'un réseau de 38 000 points de vente qui appartiennent à des intermédiaires commissionnés. Et en matière de lutte contre la fraude, on ne procède pas comme si c'étaient des collaborateurs.

Dans cette activité, il y a 30 millions de clients. Et, contrairement aux vôtres, ce sont des clients anonymes, sauf ceux qui jouent sur Internet. Prévenir la fraude, notamment de la part des joueurs – parce que la fraude vient surtout des joueurs – quand ils sont anonymes, c'est compliqué.

A l'image de ce qui se fait dans l'assurance, les produits sont essentiellement dématérialisés.

La Française des jeux est donc une grosse PME par les effectifs, mais avec des problématiques, si je puis dire, de grande entreprise, notamment de par les flux financiers que l'on collecte dans l'année pour le compte de l'Etat.

Concernant la typologie de fraude, il y a **trois groupes** : **les fraudes qui viennent des clients**, donc de nos joueurs ; ce sont des risques de fraude informatique, puisque nos produits, pour tout ce qui n'est pas jeux de grattage, sont des combinaisons informatiques traitées sur des gros systèmes. Il y a des fraudes qui sont des **contrefaçons sur les tickets** de jeux de grattage. Et bien sûr, la dernière-née, mais pas la moindre, **la fraude sur les jeux sur Internet**. Une catégorie à part est le **poker en ligne**.

Le deuxième groupe, ce sont les fraudes là aussi historiquement appelées internes, les fraudes qui sont le fait de collaborateurs ou du réseau de vente. Autant à La Française des jeux, les gens sont sensibilisés aux fraudes qui viennent des joueurs, autant, tout ce qui est fraude interne reste un sujet tabou, et on a du mal à leur en faire prendre conscience. Cela va de la fraude classique sur les processus opérationnels – comme dans toutes les entreprises – à des fraudes un peu plus évoluées dans le réseau de points de vente, avec subtilisation de reçus de jeu. Et enfin, tout ce qui est fraude possible sur les systèmes de tirage.

Le troisième groupe est le blanchiment, mais là, c'est une affaire de spécialistes.

Romain MARIE

On peut poursuivre avec les dispositifs que vous avez été amenés à mettre en place compte tenu d'une structure qui, comme vous le disiez, n'est pas très grande. Combien de collaborateurs, en tout ?

Valérie BERCHE

Neuf cent cinquante. Et, comme je le disais, dans une société très sensible à tout ce qui est sécurité et intégrité du jeu. Il faut dire que, sur les neuf cent cinquante personnes, plus du tiers de celles-ci sont des informaticiens. La sécurité et l'intégrité des jeux, et les fraudes qui peuvent en découler sont des réflexes de couverture chez nous.

Depuis longtemps, on a mis en place des systèmes de surveillance. Mais ces systèmes de surveillance présentaient des lacunes. L'organisation a consisté à recenser tous les systèmes de surveillance et de contrôle qui pouvaient exister pour couvrir l'intégralité des activités diverses que je vous ai exposées. Et là, l'audit interne a été le bras armé, si je puis dire, de la direction générale pour poser les principes de la politique fraude de l'entreprise.

Comment devenir proactif dans la gestion de la fraude ?

Il a été décrété officiellement que la sécurité et le contrôle interne devaient être au cœur des préoccupations. C'est beaucoup plus facile à dire qu'à faire, surtout dans un secteur qui s'ouvre à la concurrence, avec une dualité monopole et concurrence qui n'est pas simple à gérer ; on change de monde et d'environnement. Il faut, en outre, faire appréhender aux opérationnels le risque croissant lié à la fraude, ce qui est excessivement compliqué. Cette politique de prévention de fraude a commencé à être mise en place avec une action très forte des dirigeants et des instances de gouvernance qui se sont dites impliquées dans la prévention de la fraude, et ont promulgué un code éthique. Il faut faire savoir les actions de surveillance et de contrôle existantes dans l'entreprise ; adapter les délégations de pouvoirs en conséquence. La communication a un rôle de sensibilisation en interne et dans le réseau de points de vente. Concernant la mise en œuvre, on a urbanisé les systèmes de surveillance et de contrôle, avec un audit interne qui assure, comme d'habitude, un contrôle périodique, mais qui aide aussi à coordonner les périmètres des entités de contrôle, parce que les opérationnels doivent travailler, produire du chiffre d'affaires, et non pas étouffer sous les contrôles, comme on l'a parfois vu.

Les périmètres ont donc été répartis de façon extrêmement précise. La surveillance des 38 000 points de vente, où l'on trouve les fraudes liées au blanchiment, est assurée par des inspecteurs réseau qui tournent en permanence ; ils dépendent de la direction de la sécurité qui a à sa tête un ancien de la DGSE.

Romain MARIE

Combien sont-ils, pour 38 000 points de vente ?

Valérie BERCHE

Aujourd'hui, une quarantaine : neuf inspecteurs réseau qui sont d'anciens gendarmes ou d'anciens assureurs, et 35 personnes qui se consacrent à la surveillance du réseau physique, pour une partie, et du réseau multimédia, qui sont des processus différents. Ces personnes gèrent également les incidents, les fraudes quand elles sont avérées, et les crises.

L'informatique est un élément fondamental de toute cette surveillance. Vingt personnes assurent la sécurité des systèmes d'information, et il y a trois cents informaticiens en tout. Ces vingt personnes assurent aussi bien la surveillance des 25 000 terminaux qui sont en points de vente que la surveillance en interne. Ils sont sensibilisés à tout ce qui peut être attaque en interne, notamment l'accès à des fichiers extrêmement sensibles comme celui des lots non réclamés.

Telle est l'organisation, avec une coordination pour compte de la direction générale, de l'audit interne sur l'ensemble des périmètres de contrôle et de surveillance.

Romain MARIE

Marc Fourrier, dans le secteur de l'assurance, vos produits sont distribués à travers un réseau d'intermédiaires. Comment contrôle-t-on un réseau de distribution ? Pouvez-vous nous donner un exemple de dysfonctionnement ?

Marc FOURRIER

Dans l'activité d'assurance, on ne vend rien de bien concret, à vrai dire. On est dans l'activité d'épargne, un peu comme les banquiers ; donc on collecte de l'information, on conseille les clients et on leur vend des produits correspondant à leurs besoins. Ou bien on est dans le domaine de

l'assurance ; les gens paient des primes pour avoir le droit de faire réparer un dommage qui interviendra avec une probabilité que personne ne connaît.

Toute notre activité est basée sur la confiance des clients. Le pire pour nous, c'est d'être confrontés à des fraudes qui mettront à mal cette confiance.

Nous travaillons, en matière de distribution, avec des réseaux d'intermédiaires. Ils peuvent être salariés, agents généraux, courtiers, dans la distribution en direct. Cela représente à peu près dix mille personnes réparties sur tout le territoire.

Ce qui peut arriver, le plus dangereux pour nous, c'est qu'un intermédiaire de chez nous ou un intermédiaire autre, collecte des primes et ne les envoie pas à la compagnie. Le client est persuadé d'être assuré, il a un document à en-tête de la compagnie, mais en fait, il ne l'est pas. Si l'on ne fait rien, on se retrouve soit avec un dommage, soit avec une personne qui vient nous voir, à un moment donné, pour qu'on lui restitue son argent ou qu'on lui règle un sinistre, et l'on est obligé de constater que cette personne n'est pas cliente et qu'elle n'est pas couverte pour le risque en question. Le pire est de se retrouver dans la presse avec une couverture média non voulue. Cela arrive de temps en temps à toutes les compagnies.

Dans ce cas-là, que faisons-nous, comment pouvons-nous détecter la fraude plus vite ?

Le problème est que, quand un détournement de fonds est effectué par un intermédiaire, s'il monte bien son affaire, on n'en saura rien. On n'en saura rien tant que le client ne réclame pas. On va donc commencer par mettre au point un système d'identification des réclamations clients extrêmement performant. Vous me direz : le client n'est pas obligé d'alerter la compagnie, il peut appeler son intermédiaire, le fraudeur. Cela arrive aussi. Mais au bout d'un moment, quand il n'est pas satisfait des réponses, il appelle la compagnie. On doit être capable de détecter, avec des signaux parfois assez faibles, que ce n'est pas une réclamation commerciale, car il ne faut surtout pas la renvoyer sur le commercial, ce qui risquerait de créer une escalade et des problèmes mal maîtrisés. Comment peut-on détecter plu vite – c'est toujours notre problématique – des cas anormaux ? On est là dans l'activité normale de surveillance d'un réseau de distribution, avec l'analyse des écarts ou des situations anormales, comme de très grosses productions qui arrivent subitement, ou des chutes de production inexpliquées. Cela nécessite donc, de la part des managers de proximité, des actions très concrètes d'analyse.

Dès lors que des clients sont lésés, le risque de médiatisation, comme je l'ai dit, est assez élevé. Nous avons donc mis en place un système de cellule de crise capable de se réunir quasi instantanément, avec une politique de communication pour des cas mettant en jeu des sommes relativement importantes. La position de la compagnie est déjà arrêtée et on sait qui va aller, face à un micro, parler aux journalistes, passer à FR3, etc. On s'est organisé de façon à ne pas laisser place à l'improvisation, face aux médias.

Romain MARIE

Au sein de France Télécom, vous avez des dispositifs, j'imagine, mis en place pour lutter contre le *hacking*. Je pense que la réactivité doit être primordiale dans vos activités.

Michel LAPORTE-MARROUX

Même sans parler de *hacking*, qui est un moyen particulier pour le fraudeur d'accéder à nos services, aux produits, je dirai que, d'une manière générale – encore une fois pour simplifier la chose –, on est face à des problèmes de cybercriminalité ou qui présentent les mêmes caractéristiques.

La réactivité et l'anticipation sont donc très importantes. Malheureusement, le fraudeur a bien souvent une ligne d'avance. Par contre, grâce à un réseau d'*intelligence*, une activité de veille, qu'elle soit en interne ou en externe, il est possible de partager, de mutualiser à différents niveaux.

Pour l'externe, France Télécom est présent dans de nombreux organismes professionnels qui réglementent plus ou moins, ou structurent l'activité des télécoms dans le monde, surtout pour l'activité mobiles. Il y a une équipe ad hoc, des ateliers de travail consacrés à la lutte contre la fraude. C'est l'occasion de partager des expériences, en huis clos, entre professionnels, et donc de pouvoir anticiper.

En matière de veille, il y a aussi tout simplement le suivi de la presse, qu'elle soit professionnelle ou générale, dans laquelle on trouve des informations qui permettent d'attirer l'attention sur des problèmes auxquels nous pourrions être exposés. Cela donne toujours lieu à une analyse en interne, parfois à une transposition dans notre secteur d'activité pour essayer d'anticiper et de comprendre ce qui est peut-être déjà malheureusement un acte de fraude installé.

En veille interne, nous nous appuyons sur un réseau de trois cents collaborateurs qui sont principalement affectés à la lutte contre la *fraude et le revenu assurance*. Chaque fois qu'un événement se passe dans le monde, chez un de nos opérateurs, un flux d'informations nous rapporte ces incidents. Nous sommes parfois amenés à aller sur place pour effectuer des recherches, comprendre un peu mieux, et être ainsi capable de faire des recommandations et de les diffuser à l'échelle du groupe. Cela donne lieu à des alertes très fréquentes, parfois d'heure en heure, ou de jour en jour. Par exemple, quand nous détectons une destination à tarif très élevé, un numéro spécial surtaxé, qu'un fraudeur vient d'ouvrir, peut-être en Italie ou en Corée du Nord, lieu propice pour ce type de fraude, nous diffusons cette information, de façon à ce que nos équipes et filiales puissent sinon suspendre cette destination, au moins la mettre sous surveillance.

Une autre partie de la veille concerne les travaux en laboratoire. L'idée est de penser et d'agir comme un fraudeur, de conduire parfois des attaques sur nos réseaux ou infrastructures, en les simulant en laboratoire ; parfois, c'est juste de reproduire ce qu'un fraudeur a fait sur le terrain, pour essayer de comprendre toutes les actions qu'il a pu entreprendre.

Une fois que l'on dispose de tous ces renseignements, que ce soit dans la cartographie des risques ou dans d'autres supports de communication, il est important de diffuser et d'animer tout le réseau de façon à ce que ces choses-là soient comprises, et que les actions soient entreprises. On a mis en place un programme CAT : *Communication, awareness & training*. C'est un ensemble de supports et d'interventions, sur le terrain ou à distance, avec différents supports (audio, vidéo), qui permettent à l'ensemble de nos interlocuteurs – soit les correspondants *Fraud & Revenue assurance*, soit les experts techniques du réseau, des systèmes d'information – de comprendre les problèmes, de mesurer les impacts à l'échelle de leur activité ou de l'entreprise, de l'entité, et également de prendre des décisions et de déployer des actions pour résoudre le problème, le supprimer ou au moins le mettre sous surveillance.

Pour aider les personnels dans la prise de décisions et le déploiement des solutions, nous les accompagnons d'un point de vue opérationnel dans la définition des contrôles, la conduite des plans d'action, la coordination ; nous accompagnons également les équipes *Fraud & Revenue assurance* sur place, pour sensibiliser leur management à tout ce qui est problématique, comme les impacts financiers.

Nous travaillons en très forte collaboration avec les fournisseurs de solutions, lutte contre la fraude et sécurisation des flux de revenus.

Romain MARIE

Mme VAN DER LINDEN, peut-être pouvez-vous nous indiquer comment vous faites pour rechercher aussi des dysfonctionnements dans votre organisation ? Comparer peut-être des indicateurs ?

Catherine VAN DER LINDEN

Pour revenir au risque de détournement d'actifs physiques, qui est un point peut-être plus sensible dans le secteur industriel, je dirai tout d'abord qu'il faut bien solliciter et écouter attentivement les opérationnels et les financiers sur les indicateurs qui leur semblent pertinents et les bonnes mesures de la marche normale des activités. On s'aperçoit en fait qu'en travaillant avec ces spécialistes, on peut identifier avec eux les anomalies entre l'évolution des paramètres et les paramètres financiers par rapport à ces indicateurs de référence qui peuvent être, en fait, des moyens assez intéressants et puissants de détection, au moins d'anomalies, voire de fraudes.

Les incohérences, par exemple, entre des sorties de dépôt, et des quantités effectivement passées dans les comptes, sont des choses assez basiques et assez simples à mettre en œuvre ; les incohérences entre des niveaux de consommation, des heures d'intervention, des niveaux de tonnage effectivement manipulés, transcrits dans les registres opérationnel et financier, peuvent aussi permettre de détecter des signaux faibles d'anomalies et parfois des vrais détournements d'actifs. Des éléments très simples qu'il faut rapprocher, peuvent être assez puissants.

Nous avons fait une revue, dans notre groupe, avec la logistique et la finance sur la gestion de la matière – matière, pour nous, c'est le pétrole, les produits pétroliers –, le flux d'une raffinerie jusqu'au consommateur final (et il y a beaucoup d'échelons dans ce processus), en identifiant, avec les opérationnels, les logisticiens, les financiers, les types de risques de détournement de produits. Nous avons déterminé avec eux des dispositifs de prévention dont ils sont souvent les créateurs. Nous sommes souvent simplement des catalyseurs de la réflexion vis-à-vis des opérationnels.

Romain MARIE

Puis-je vous demander ce qu'est, chez vous, une fraude majeure, par exemple ? Peut-on valoriser ?

Catherine VAN DER LINDEN

Bien sûr, on peut toujours valoriser, mais je ne pense pas qu'il faille trop communiquer au sein des groupes sur le niveau acceptable, le montant acceptable. Il y a bien sûr des niveaux plus ou moins significatifs, et des éléments qui peuvent mettre en risque une entreprise et d'autres pas. Mais il y a un aspect de communication de tolérance 0, me semble-t-il, qui reste souhaitable.

Et dans les domaines de gestion d'actifs physiques, 1 + 1 + 1, à la fin, cela fait beaucoup.

Romain MARIE

Pardonnez ma curiosité d'auditeur.

Chez Alstom, j'estime une fraude majeure au-dessus de cinq millions d'euros. Voilà ce que je considère comme étant une fraude majeure, que je mets en regard des politiques d'assurance en vigueur dans le groupe.

Je crois, en outre, qu'il ne faut pas trop considérer la fraude comme un tabou, et qu'il vaut mieux en parler.

Catherine VAN DER LINDEN

Je suis tout à fait d'accord.

Comment devenir proactif dans la gestion de la fraude ?

Romain MARIE

Mme BERCHE, peut-être pouvez-vous me donner quelques exemples de dysfonctionnements chez vous, des exemples concrets, récents ou pas récents, c'est toujours intéressant.

Valérie BERCHE

Cela restera très secteur jeux, donc vraisemblablement assez atypique par rapport à ce que vous pouvez connaître, mais j'ai beaucoup apprécié ce que vous disiez tout à l'heure, M. Sautin, sur la connaissance des opérationnels.

Je peux parler d'une fraude qui, de mémoire, s'est produite en 2006, puisqu'elle a été médiatisée. On l'a appelé la fraude de la rue des entrepreneurs, car elle concernait un point de vente du 15e arrondissement. Un gagnant se présente. A la Française des jeux, au-delà d'un certain montant, il est convié, avec champagne et petits fours, pour remise de son gain par la direction générale et toujours en présence de l'entité qui, chez nous, est responsable des gros gagnants. Ce n'est pas pour leur indiquer des placements, vous pensez bien, mais il s'agit d'une véritable prise en charge psychologique sur plusieurs semaines, voire plusieurs mois après le gain, parce que, des études le prouvent, gagner une grosse somme d'argent subitement transforme quiconque. Dans ces études extrêmement sérieuses, il y a des profils types de gagnants. Tout le monde entre dans une catégorie profil type. Et, la responsable service, quand elle a vu ce gagnant, elle l'a trouvé – je cite – « bizarre ».

Qu'est-ce qu'un gagnant bizarre ? En l'occurrence il s'agissait d'une personne extrêmement agressive, arrogante, impatiente, poussant presque le président de l'entreprise à signer rapidement, rechignant à dire son nom ; et malgré tout il faut bien mettre un ordre.

Bref, il était bizarre. Néanmoins, il avait entre les mains le fameux reçu de jeu, qui est un titre au porteur, donc totalement anonyme. Souvenez-vous, les joueurs sont anonymes, donc les gagnants par essence aussi. Il avait le reçu, reçu validé, survalidé, revalidé dans notre informatique. Il a donc fallu lui donner ses chèques, à contrecœur, je ne vous le cache pas. Mais on ne pouvait absolument rien faire.

Le hasard faisant bien les choses parfois, la banque nous appelle : nos relations avec les agences bancaires sont fréquentes, notamment en raison du blanchiment. Et la banque nous demande: « Sur cette personne, on voudrait savoir si vous avez des informations, etc. ? » On est là dans le prétraitement de la fraude : par sécurité, la direction de la sécurité dépose plainte. On ne sait jamais, cela peut servir.

On travaille très régulièrement avec la police. On dépose plainte et on met le détaillant, chez qui la prise de jeu a été faite, sous surveillance. Je ne vous dis pas comment on fait, parce que c'est devenu depuis un élément fondamental. Grâce à ce détaillant, nous avons beaucoup appris...

On s'est aperçu, grâce à la surveillance, que la combinaison qui avait fait l'objet du gain continuait à être jouée tous les lundis matin entre 8 heures et 9 heures. Ce n'est pas une histoire que je vous raconte, c'est la réalité. Et on sait, par expérience, qu'un joueur qui gagne gros arrête de jouer la même combinaison, parce qu'il se dit intuitivement qu'elle ne ressortira plus. A partir de là, la police a mis en place un système de surveillance et, dans l'enquête policière, on a retrouvé le vrai gagnant. La fraude a donc été établie vis-à-vis du détaillant, et bien sûr, l'agrément lui a été retiré immédiatement.

Romain MARIE

Merci beaucoup pour cette réponse très complète.

M. LAPORTE-MARROUX, peut-être un exemple de dysfonctionnement au sein de votre organisation ?

Michel LAPORTE-MARROUX

Je vais parler de *Interconnection bypass*, que l'on appelle en français « revente d'appels ». Il faut savoir que tous les réseaux de télécommunications sont heureusement interconnectés et que tout appel naissant dans un réseau, que vous générez pour joindre un client de Bouygues Télécom ou SFR, permet à l'opérateur qui reçoit l'appel d'encaisser un revenu de l'ordre de quelques centimes par minute. C'est le revenu d'interconnexion.

Le fraudeur va acheter des cartes SIM, des mobiles de l'opérateur qu'il veut attaquer. Prenons la situation de Orange. Le fraudeur achète des cartes SIM Orange, les met dans un système informatique, dans des *racks* – c'est assez compliqué à expliquer – qui vont simuler un téléphone, qui vont permettre une communication entre la carte SIM du téléphone et notre réseau pour atteindre nos autres clients.

Il va ensuite revendre des minutes d'appel vers Orange, à des tarifs inférieurs à notre revenu d'interconnexion. On perd donc ce revenu et, grâce au marché parallèle sur lequel il vend ces minutes d'appel, il encaisse le revenu directement, soit auprès d'opérateurs peu scrupuleux qui se soucient assez peu de respecter la régulation ou l'éthique sur notre marché, soit auprès de ces petites boutiques que vous pouvez voir dans certaines rues, qui proposent des services de fax, ou de petites cabines téléphoniques. C'est un point de revente facile à trouver pour les revendeurs.

Ce que le fraudeur exploite parfois, ce sont des erreurs de tarification dans notre système de facturation : erreur dans la mesure de la durée d'un appel, erreur de prix, ou de décompte d'unité dans un forfait. Il a trouvé cette défaillance dans notre système ou nos processus, il va donc l'exploiter, puisqu'il ne paie pas le vrai prix complet au bon prix ou à la bonne durée. Il peut revendre et se faire une marge sur les marchés secondaires. Une autre possibilité est tout simplement, grâce au *hacking* de nos systèmes d'information, de ne payer absolument rien.

En termes de moyens de détection, il y a des outils, soit faits maison – des requêtes sur le *datawarehouse Business Intelligence* – , soit des outils que l'on trouve sur le marché, avec des critères basés sur le comportement moyen d'un utilisateur, le nombre d'appels par heure, par jour, etc., qui permettent de détecter ce type de fraude.

On peut imaginer aussi que le fraudeur ne se déplace pas avec ses *racks* informatiques et son système dans sa voiture pour faire le tour de Paris. Ce sont donc plutôt des mobiles qui, curieusement, sont fixes. C'est un moyen de détection.

Mais le fraudeur, une fois attrapé, passe évidemment sur un autre modèle, d'autres systèmes beaucoup plus évolués. Et plus on le détecte, plus il va loin dans la simulation. C'est donc toujours une problématique de temps réel, que de suivre les évolutions à sa disposition.

Romain MARIE

Le dernier thème de notre table ronde est l'implication des managers dans la lutte contre la fraude.

Mme VAN DER LINDEN, un témoignage ?

Catherine VAN DER LINDEN

Dans l'industrie, le sujet de la fraude est peut-être encore un peu tabou.

La raison en est peut-être, parmi différentes hypothèses, que l'enjeu financier des fraudes est perçu – parfois à juste titre, et parfois à tort – comme marginal par rapport à d'autres risques

économiques à gérer par l'entreprise. Indirectement, cela veut donc dire moins d'attention, moins de proactivité impulsée par le *top management*.

Il y a souvent, dans les entreprises industrielles, une implication forte effective en ce qui concerne les principes de comportement globaux, mais inévitablement moindre dans la détermination des modalités concrètes de maîtrise des risques de fraude, parce qu'elles sont très multiformes, qu'elles sont plutôt du domaine de la gestion terrain et que du coup, c'est parfois perçu comme un peu loin des enjeux stratégiques du *top management*.

Il y a donc finalement parfois, dans les industries, une certaine déconnexion entre le *top management* du groupe, très stratégique, et les managers terrain, qui étant très au contact des réalités au jour le jour, sont souvent beaucoup plus preneurs, attentifs et vigilants sur ces domaines.

Le cheminement recommandé, comme il l'a d'ailleurs été cité au cours de la journée, est vraiment celui utilisé dans l'industrie en matière de sécurité industrielle : avoir des objectifs volontaristes en matière de prévention, c'est clair ; sensibiliser à tous les niveaux ; et valoriser – ce n'est pas toujours gagné – le recensement, l'analyse systématique des risques en cas d'accident, et de presque accident, parce que je pense qu'il est aussi important d'évoquer cela.

Des tentatives de fraude qui ont échoué grâce à l'entreprise, grâce à l'intervention des collaborateurs, c'est un instrument de motivation interne, à la fois un retour d'expérience à faire, mais aussi un élément d'utilisation pour la motivation interne des collaborateurs et du management. Et il faut entretenir la vigilance de tous par les retours d'expérience.

Romain MARIE

M. Fourrier, un témoignage complémentaire : rencontrez-vous également les mêmes difficultés dans votre structure ; d'autres difficultés ?

Marc FOURRIER

Ce métier est forcément très différent. En fait, le monde de l'assurance – et de la banque, d'ailleurs – est un métier de risque. On prend des risques et on construit les produits sur une base d'analyse de risques. Il y a donc déjà cette culture risque. Je parlais de la dichotomie fraude interne/fraude externe. La fraude à l'assurance existe depuis que l'assurance existe, elle est donc complètement intégrée dans les pratiques et dans les processus.

En revanche, sur la fraude interne, c'est un peu différent. Quelque chose nous a aidés ou nous aide dans la réglementation Nous sommes une activité extrêmement réglementée, que ce soit sur la banque, avec Bâle II, et *Solvency* II sur l'assurance.

Il est affiché maintenant que, en matière de *compliance*, dans la lutte contre les grandes familles de risques, la fraude interne et la fraude externe sont des priorités. Mais cela est assez récent.

En 2006, quand on a créé cette coordination de la lutte antifraude, autant la fraude à l'assurance faisait partie du quotidien du traitement, autant la fraude interne était en effet quelque chose de tabou.

Donc, la première action est en effet de convaincre, à l'échelon CEO, au niveau le plus élevé, que la fraude interne est un vrai enjeu. Nous avons été aidés par la conjoncture (nous avons eu quelques cas significatifs), par les travaux de Sarbanes-Oxley, par les débuts de *Solvency*.

Dans les délégations de pouvoir des dirigeants, il y a des clauses concernant la conformité, et la fraude interne fait partie de la conformité. Ils ont donc obligation de s'en occuper. Mais cela ne suffit évidemment pas. Il faut effectuer tout un travail de communication en interne, en faisant en sorte que les dirigeants soient les sponsors du programme antifraude, sinon, les chances de réussir sont

faibles. Nous avons créé un forum éthique en invitant le CEO, le CFO, etc., à parler de fraude, à parler de corruption, à parler de ces sujets-là aux managers.

Comme nous sommes dans une activité de risque, l'aspect évaluation des risques fait aussi partie du travail quotidien. L'aspect cartographie, évaluation des risques a eu un énorme impact pédagogique, parce que l'on a évalué des risques sous l'angle fraude, pas seulement sous l'angle erreur ou dysfonctionnement, mais sous l'angle acte volontaire de personnes à l'intérieur de l'entreprise pour frauder l'entreprise ou les clients. Cet exercice a lieu chaque année, en termes de revue, mais la première phase, la mise en œuvre, qui se fait plutôt par une approche *bottom-up*, a été extrêmement fructueuse pour sensibiliser au risque de fraude.

Nous avons développé, depuis quelque temps, des analyses proactives de détection d'anomalies susceptibles de révéler des fraudes. Nous faisons savoir à l'intérieur de l'entreprise que ces dispositifs existent. Nous ne faisons pas de la surveillance de salariés, même si nous sommes amenés à chercher, à détecter les transactions anormales par rapport à des procédures documentées. Tout le monde sait qu'il existe une activité de détection, et cela a aussi un côté dissuasif.

La fraude n'est donc plus un tabou aujourd'hui.

Romain MARIE

On pourrait dire la même chose à la Française des jeux ?

Valérie BERCHE

Ça n'est plus un tabou ? Oui, dans les entités de contrôle, on milite tous, de fait, pour la sensibilisation et même la formation, avec des exercices. Tout comme on simule des incidents et des crises, on simule des cas de fraude pour sensibiliser, très concrètement et par l'exemple, les managers.

En ce qui me concerne, je suis, non pas pour divulguer les schémas de fraude au grand public, mais au moins aux managers, en faire même des modules. Mon projet, sur l'année 2011, est d'intégrer un module prévention de la fraude dans tous les séminaires de formation récurrents des managers, ce qui est en lien avec le *top management* et ce que je disais tout à l'heure, les délégations de pouvoir.

Les services ont compris, depuis quelques années, que le contrôle interne, ils en étaient les premiers responsables. La maîtrise des activités, c'est donc leur responsabilité, et la couverture du risque, et notamment du risque de fraude dans leur activité, leur incombe également.

QUESTIONS/REPONSES

Question de la salle

Ma question concerne davantage le monde latin que le monde anglo-saxon.

Le premier obstacle à la lutte contre la fraude n'est-il pas culturel ? Je voudrais illustrer mes propos en me référant à un hold-up de neuf millions d'euros commis il y a quelques mois. A peine quelques heures après la diffusion de cette information, des dizaines de milliers d'internautes ont spontanément envoyé des mails de félicitations à ce voleur.

Comment lutter contre la fraude dès lors que le fraudeur peut parfois être un héros ?

Catherine VAN DER LINDEN

Comment devenir proactif dans la gestion de la fraude ?

Je pense qu'il ne faut pas entrer dans ce jeu-là… En tant qu'entreprise, notre rôle est de casser les envies des tricheurs et des Arsène Lupin… je ne sais pas s'il faut le dire comme cela ! (rires)

Romain MARIE

Les *Mémoires d'un tricheur*, de Sacha Guitry, ne sont normalement pas le livre de chevet des auditeurs et des contrôleurs internes.

Je tiens vraiment à vous remercier pour cette journée. Je remercie bien sûr l'IFACI pour l'organisation du colloque, particulièrement Elisabeth Weiss ; ACL, qui a été sponsor de notre colloque ; et puis tous les intervenants, dont les présentations ont été très bien préparées.