ifaci

institut français de l'audit et du contrôle internes

Cahier de la Recherche

L'audit de la fraude dans le secteur bancaire et financier

Réalisé par le Groupe Professionnel Banque

L'IFACI est affilié à The Institute of Internal Auditors

Dans la même collection

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

Pour plus d'informations : www.ifaci.com

© IFACI – Paris – janvier 2010

ISBN : 978-2-915042-24-5 – ISSN : 1778-7327

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

Préface

La fraude a toujours été un risque « endémique » dans les activités bancaires et financières, puisqu'il y est question d'argent. C'est un risque grave, car il touche au fondement même de ces activités, qui est le principe de confiance. La fraude ruine la confiance interne, indispensable à tout travail en équipe, et ruine la confiance externe, celle des clients en particulier.

Elle est dès lors un risque particulièrement coûteux, parfois directement, car des cas de fraudes portant sur des montants considérables ont été rencontrés, mais également indirectement, au travers du risque d'image et de toutes les conséquences qui peuvent lui être associées. Un établissement de crédit qui connaît des fraudes non décelées et/ou non combattues connaîtra une amplification du phénomène, car la fraude appelle la fraude, et sera victime de multiples dommages collatéraux, pouvant aller jusqu'au procès pénal et à des campagnes médiatiques aux effets désastreux.

C'est pourquoi le risque de fraude a toujours été pris très au sérieux par les banquiers. Historiquement, c'est bien entendu dans la banque de détail que les premières mesures de lutte contre la fraude ont été prises : contrôles quotidiens des mouvements comptables liés aux opérations clientèle ou aux opérations internes, rotation obligatoire des responsables d'agences selon une périodicité assez brève, organisation des tournées d'inspection dont les premières tâches consistaient souvent à pointer les factures et les stocks.

Mais la fraude se rencontre dans toutes les activités bancaires et financières, et les opérations de banque privée et de gestion d'actifs, dans lesquelles la relation de confiance peut être encore plus forte qu'ailleurs (quand un client donne mandat à son chargé d'affaires), ainsi que les activités de banque de financement et d'investissement, sont aujourd'hui tout autant concernées. Il est clair qu'avec la sophistication des techniques bancaires, en particulier dans les opérations de marché, la montée en puissance des échanges électroniques en temps réel et, de manière plus générale, avec le rôle désormais central de l'informatique dans les banques, le risque de fraude a pris des formes et une ampleur nouvelles. Les sommes en jeu peuvent alors atteindre des montants tout à fait colossaux, ainsi que certains exemples français ou étrangers l'ont montré au cours de la présente crise.

© IFACI

De fait, le temps de la crise accroît incontestablement le risque de fraude. Fragilisation des clients et des personnels, qui connaissent parfois eux-mêmes ou autour d'eux des difficultés financières, tension qui peut se traduire par des pressions fortes pour obtenir des résultats et, plus généralement, possible relâchement de certains contrôles dû aux multiples autres vérifications auxquelles il faut accorder la priorité pour préserver les résultats autant que faire se peut, peuvent conduire le fraudeur à développer l'idée que la période est propice à agir ou, à l'inverse, s'il a déjà commis une fraude, qu'il ne peut plus revenir en arrière. C'est le syndrome bien connu dans les affaires les plus récentes de la « fuite en avant ».

Dans ce contexte, le régulateur se préoccupe depuis longtemps du risque de fraude et a pris des dispositions qui se sont renforcées au fil du temps, particulièrement au cours de la période récente. Ainsi, sous l'angle quantitatif, le risque de fraude a été intégré aux risques opérationnels qui doivent être traités dans le Pilier 1 du ratio de solvabilité. C'est reconnaître que ce risque est inéluctable dans le domaine bancaire et financier et qu'il faut d'emblée savoir le mesurer et le couvrir par un montant de fonds propres approprié. Mais au-delà du quantitatif, des efforts qualitatifs ont aussi été demandés aux établissements, au travers de leur système de contrôle interne. Et après l'énorme perte subie par la Société Générale début 2008, plusieurs textes ont été adoptés ou renforcés pour lutter contre le risque de fraude.

A ce titre, il faut partir du point de vue que ce risque concerne tout le monde au sein de l'organisation et qu'il ne peut y avoir de fraude si le fraudeur ne décèle pas une opportunité de frauder et si les outils et procédures ne comportent pas des failles, techniques ou, encore plus simplement, humaines. La force de l'habitude ou la crédulité sont des facteurs qui favorisent le risque de fraude tout autant que la complexité de certains processus techniques et informatiques. Le cadre de contrôle interne doit donc impliquer tous les processus et tous les acteurs de l'entreprise, du plus haut au plus bas. Des mécanismes d'alerte du bas vers le haut doivent également être établis. C'est pourquoi le recensement et la remontée des incidents ont fait l'objet de dispositions ad hoc au sein des récentes modifications réglementaires.

Au total, les établissements doivent promouvoir deux aspects fondamentaux d'une même culture. L'intégrité, tout d'abord, car elle est indispensable pour générer la confiance intrinsèque aux activités bancaires et financières. Mais l'intégrité est une qualité humaine, que l'on peut préserver voire encourager par des politiques adaptées de rémunérations et d'évolution professionnelle des personnels, mais qui ne dépend pas que de l'entreprise : le contexte politique, culturel, social peut influer sur le compor-

© IFACI

tement de tout un chacun, malgré les efforts de l'entreprise. Il faut donc développer également la culture du risque.

L'auditeur tient une place centrale dans cette culture du risque. Bien entendu, il n'est pas seul et les dirigeants, tout comme les contrôleurs permanents, ont un rôle également essentiel. Mais, par son exemplarité, par sa capacité à sensibiliser les personnels, au travers des contrôles qu'il effectue, l'auditeur apporte une pierre solide à l'édifice, car il participe ainsi à la prévention du risque.

En matière de risque de fraude, comme pour bien d'autres choses, l'adage nous enseigne qu'il faut mieux prévenir que guérir. Le cahier de l'IFACI sur l'audit de la fraude dans le secteur bancaire et financier participe de cet effort. Il donne maintes références et apporte des réponses pratiques aux questions que se posent les auditeurs confrontés à l'appréhension du risque de fraude. En présentant les typologies de la fraude, en évoquant les possibles structures organisationnelles et les différentes techniques de lutte adoptées au sein des établissements, ce cahier fourmille d'exemples qui devraient permettre à tous de progresser. Avec sa perspective internationale, et ses conseils pratiques compte tenu des risques juridiques que peuvent impliquer certaines méthodes de lutte contre la fraude, il est également un outil précieux qui peut éviter bien des erreurs.

A l'instar des autres cahiers thématiques déjà publiés dans cette collection, il devrait rapidement devenir un outil de référence pour tous les auditeurs.

Dominique LABOUREIX
Directeur de la Surveillance Générale du Système Bancaire
Secrétariat général de la Commission Bancaire

© IFACI

Remerciements

L'IFACI tient tout particulièrement à remercier les membres de l'Unité de Recherche qui, sous la responsabilité de **Frédéric GEOFFROY**, ont conçu et rédigé ce cahier :

Jean-Pierre BOUCHART, *Associé, PricewaterhouseCoopers Audit ;*

Cécile CHARLES, *Auditeur interne, La Banque Postale ;*

Frédéric GEOFFROY, *Responsable Audit SGIB, Société Générale ;*

Stéphane GUILLEAUME, *Directeur de l'audit, Group Audit France ABN AMRO ;*

Béatrice KI-ZERBO, *Directeur de la Recherche, IFACI ;*

Céline ROY-LARENTRY, *Associé, PricewaterhouseCoopers Audit ;*

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

Sylwia PYZIAK, *Inspecteur, Inspection générale, Société Générale ;*

Inès de ROLLAND, *Business Auditeur SGIB, Société Générale ;*

Anne-Marie SCHRICKE, *Responsable relations régulateurs, Inspection Générale, Calyon ;*

Jonathan STROCHLIC, *Business Auditeur SGIB, Société Générale ;*

Ces travaux s'insèrent dans le cadre du **Groupe Professionnel « Banque » de l'IFACI** présidé, en 2009, par **Patrice JOSNIN,** *Responsable adjoint de l'Inspection, BNP Paribas,* et composé de :

Yves CAPLAIN, *Inspecteur Général, La Banque Postale ;*

Frédéric GEOFFROY, *Responsable de l'audit interne, Banque de financement et d'investissement du groupe Société Générale (SGCIB) ;*

Christiane LEGAT, *Responsable de l'audit interne, GE corporate Banking Europe ;*

Michel LE MASSON, *Inspecteur Général, Crédit Agricole SA ;*

Claire VALTOT, *Head of Resources and Operations, Orbeo.*

L'IFACI tient également à remercier, pour leur participation à la révision et à la mise en forme de cet ouvrage :

Julie FERRE, *Assistante de la Recherche, IFACI.*

L'IFACI tient tout particulièrement à remercier **Dominique LABOUREIX,** *Directeur de la Surveillance Générale du Système Bancaire au Secrétariat général de la Commission Bancaire,* pour avoir accepté de préfacer ce cahier de la recherche.

Louis VAURS, *Délégué Général, IFACI*

© IFACI

Sommaire

Préface 3
Introduction 9

Partie I – Fraude : Définition, impacts et typologie 11
1.1- Définition 13
1.2- Les impacts de la fraude 14
1.2.1- Impact financier 14
1.2.2- Impact en termes d'image 15
1.2.3- Quelques exemples d'impact de fraude 16
1.3- Typologie de la fraude 17
1.3.1- Principaux types de fraude 19
1.3.2- Le triangle de la fraude 20
1.3.3- Profil du fraudeur 20

Partie II – Audit interne et risque de fraude : la position de l'IIA et des principaux régulateurs 23
2.1- Position de l'Institute of Internal Auditors (IIA) 25
2.2- Rappel du cadre réglementaire 27
2.2.1- France 27
2.2.2- Royaume-Uni 30

Partie III – Gouvernance et pilotage du dispositif de lutte contre la fraude 33
3.1- Les acteurs clés du dispositif 35
3.2- Le mandat et le rôle de l'audit dans le dispositif de lutte contre la fraude 36

Partie IV – Le risk assesment et les procédures d'audit de la fraude 45
4.1- Les modalités d'analyse des risques 47
4.1.1- Le risque de fraude dans le cadre d'une approche globale 47
4.1.2- Une approche plus ciblée du risque de fraude 47
4.1.3- La méthode des « scénarios » 52
4.2- Les missions d'audit et la détection de la fraude 52
4.2.1- L'audit interne : une revue périodique 52
4.2.2- Les différents cadres de contrôle et leur impact sur les contrôles anti-fraude 53

© IFACI

4.3- Les différents niveaux de contrôle 54
4.3.1- La vérification de la mise en place des contrôles opérationnels 54
4.3.2- Les contrôles spécifiques anti-fraude 55
4.4- Fraude et sécurité informatique 63
4.4.1- Répartition des incidents de sécurité en entreprise 63
4.4.2- Dommages dus au piratage informatique 64
4.4.3- Détournement des outils informatiques à des fins frauduleuses et vol d'informations stockées sur des supports informatiques 65
4.4.4- Les moyens techniques de sécurisation et de détection de la fraude informatique 66
4.4.5- Le rôle de l'audit des systèmes d'informations dans la lutte contre la fraude informatique 66
4.5- L'utilisation d'outils informatiques dans les missions d'audit de la fraude 68
4.5.1- L'extraction des données : utile et efficace sur certains types de fraudes 68
4.5.2- Le data mining dans la recherche de fraudes 69

Partie V – La conduite d'une mission d'investigation de fraude 71
5.1- La conduite de la mission 73
5.1.1- Le recueil des preuves 73
5.1.2- Les entretiens 75
5.1.3- La rédaction du rapport 77
5.2- Les aspects juridiques 77
5.2.1- Les opérations personnelles des agents 77
5.2.2- Les investigations sur les postes de travail 78
5.2.3- L'utilisation des conversations téléphoniques 79
5.2.4- L'utilisation de la vidéosurveillance 79
5.2.5- La conservation des preuves 80
5.2.6- Relations avec la police et les autorités judiciaires 80

Conclusion 82

Annexe 1 : Exemples de fraudes internes dans l'octroi de crédits 84
Annexe 2 : Type et profil du fraudeur 86
Annexe 3 : Cadre Réglementaire aux Etats-Unis et aux Pays-Bas 87

Bibliographie 95
Webographie 99

© IFACI

INTRODUCTION

La gestion du risque de fraude est un sujet qui concerne l'ensemble des organisations et chaque métier.
En ce qui concerne le secteur bancaire ou la sphère financière au sens plus large, plusieurs événements récents ont montré l'ampleur que pouvait prendre la fraude, son impact très négatif sur les comptes et l'image des établissements concernés. Les régulateurs ont marqué avec force, par des interventions et des textes récemment publiés, leur volonté de voir tous les acteurs du secteur bancaire faire de la lutte contre la fraude une priorité et s'organiser en conséquence.

C'est dans ce contexte que le groupe professionnel « Banque » de l'IFACI a constitué un groupe de travail pour rassembler les contributions de praticiens de l'audit interne venant d'horizons différents dans un cahier de la recherche.

L'objectif de cette publication est de définir le rôle de l'audit interne vis-à-vis de la fraude, de proposer une approche et des instruments pour faciliter le travail des praticiens et de répondre aux questions suivantes :

- Quelle définition et quelle réglementation ?
- Quels indicateurs et quels contrôles types ?
- Comment conduire une « mission fraude » ?
- Quels intervenants aux cotés de l'audit interne ?

Il est aussi utile de rappeler que le contrôle périodique n'est qu'un élément du dispositif de prévention et d'identification de la fraude. Son intervention est nécessaire, indispensable même, mais la prévention de la fraude la plus efficace repose aussi, et avant tout, sur une gouvernance établie qui doit se décliner depuis les instances dirigeantes les plus élevées jusqu'aux agents impliqués dans le traitement quotidien des opérations.

© IFACI

© IFACI

Partie I

Fraude : Définition, impacts et typologie

© IFACI

© IFACI

1.1- Définition

Le guide pratique sur la gestion du risque de fraude publié sous l'égide de l'IIA, de l'AICPA et de l'ACFE définit la fraude de la manière suivante :

> *« La fraude est un acte volontaire ou une omission volontaire, ayant pour objet de tromper un ou des tiers. Il en résulte une perte pour les victimes et/ou un gain pour le fraudeur »*[1]

Trois aspects de cette définition sont à souligner :

- **le caractère volontaire de la fraude,** qui la distingue de l'erreur ou de la simple négligence ;
- **la tromperie,** caractérisée par la dissimulation et/ou l'abus de position et/ou la violation de la confiance ;
- enfin, **le gain recherché par le fraudeur,** gain qui peut être matériel ou moral, atteint directement ou indirectement, pour son compte ou le bénéfice d'un proche. A noter aussi que dans le cas de la stricte malveillance, la fraude peut se traduire par une perte pour la victime sans gain tangible pour le fraudeur.

La fraude ainsi définie ne se limite donc pas aux délits usuellement réprimés par le Code Pénal (le vol, l'escroquerie, l'abus de confiance, etc.). A titre d'exemple la captation de l'héritage d'un client par un collaborateur n'est pas nécessairement un délit pénal ; en revanche elle constituera une fraude à ses obligations professionnelles et aux droits légitimes du client et des héritiers.

D'autres agissements entrent dans le cadre de cette étude, même si la qualification de fraude ne peut leur être donnée :

- **la complicité de fraude** peut être active ou passive. La dissimulation d'une fraude rend son auteur complice de la fraude. Par ailleurs, pourrait être assimilée à une complicité passive de fraude, la négligence qui lui a permis d'être perpétrée ou de se poursuivre ;
- **une tentative de fraude ou une fraude avortée** est une fraude qui n'a pas atteint effectivement l'objectif délictueux recherché ; elle est assimilée à une fraude avérée ;
- **un soupçon de fraude** est un ensemble de faits anormaux, non déclarés et/ou non autorisés, même si la qualification de fraude ne peut être établie avec certitude.

[1] *« Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator a gain ».*

© IFACI

1.2- Les impacts de la fraude

Les fraudes n'ont pas pour seules conséquences une perte de revenu et de crédibilité pour les établissements bancaires. Elles peuvent également, dans des cas extrêmes, provoquer la disparition pure et simple de l'établissement. En effet, il ne faut pas oublier les conséquences catastrophiques que peuvent avoir les engagements éventuels que le fraudeur peut avoir pris au nom de son établissement et que celui-ci devra honorer. Si la fraude n'a pas été découverte assez rapidement et que les engagements pris sont trop importants, la faillite de l'établissement n'est pas impossible. De plus, même si, dans une situation normale, la banque peut trouver aisément des moyens de refinancement, ceux-ci peuvent être limités ou trop onéreux dans la situation exceptionnelle provoquée par fraude : celle-ci révélée, les contreparties habituelles de l'établissement peuvent refuser de lui prêter les liquidités nécessaires et le dépôt de bilan devient alors la seule solution envisageable. L'exemple bien connu de la banque Barings est d'ailleurs édifiant. Les positions prises par le trader Nick Leeson avaient engagé la banque à de tels niveaux que celle-ci s'est trouvée en situation de faillite.

La fraude a donc un double impact : financier le plus souvent, mais également en termes d'image quand elle est rendue publique. Il existe d'ailleurs une corrélation entre ces deux aspects. L'atteinte aux finances de l'entité concernée altère son image dans le public et toute atteinte à l'image a un impact négatif supplémentaire sur l'activité et donc les comptes de cette entité.

1.2.1 - Impact financier

L'impact financier d'une fraude n'est pas limité à la perte d'actifs. Elle revêt des formes multiples tels que :

- la perte directe, qui peut compromettre la continuité d'activité ;
- la perte de clientèle, accompagnée éventuellement de retraits de fonds importants ;
- la chute du cours de l'action (perte de confiance) ; éventuellement, une augmentation de capital avec effet dilutif pour rétablir les fonds propres ou bien encore prise de contrôle opportuniste par un autre établissement ;
- l'exigence de capitaux normatifs renforcée pour faire face à un risque opérationnel dont la fréquence et l'impact sont revus à la hausse suite à la fraude ;
- le coût des mesures d'investigation liées à l'obligation ou à la nécessité de recourir à un cabinet externe ;
- la perte d'opportunité liée à la suspension provisoire ou définitive de certaines activités ou à la réduction des limites d'intervention ;
- le risque de procès (« class action » aux Etats-Unis) sur le fondement du préjudice subi par les investisseurs ;
- l'amende infligée par les autorités de tutelle dans les cas les plus graves ;
- le coût des mesures de remédiation.

© IFACI

Le régulateur apprécie l'impact sur les comptes d'un établissement non seulement du point de vue de l'établissement concerné et de sa solidité intrinsèque, mais aussi du point de vue de l'investisseur qui est pénalisé en raison d'une défaillance du dispositif de contrôle interne.

1.2.2 – Impact en termes d'image

L'impact en termes d'image, bien entendu étroitement lié aux conséquences financières de la fraude, n'en est pas moins considérable :

- la fraude, si elle est d'une certaine ampleur, sème le doute et mine la confiance des déposants ;
- l'attractivité de la banque auprès des candidats éventuels est également altérée ;
- les régulateurs étrangers peuvent se montrer plus réticents à accorder des licences d'exploitation à un établissement dont l'image a souffert d'une fraude majeure, dans la mesure où celle-ci traduit des défaillances graves en matière de contrôle des opérations.

Le problème d'image se pose dans tous les pays et particulièrement dans les périodes de crise économique. Si la fraude concerne des activités complexes comme les activités de banque d'investissement, cette complexité constitue un facteur d'incompréhension et de méfiance supplémentaire. Il est d'ailleurs intéressant, de ce point de vue, de noter que les banques d'investissement américaines les plus connues, comme Goldman Sachs, par exemple, considèrent que le risque d'image est le risque le plus sensible, dans la mesure où la réputation d'un établissement est longue à reconstruire après un incident majeur.

Il appartient à la direction de la communication de juguler la dégradation de l'image subie par la banque du fait de la divulgation de la fraude auprès du grand public et de la communauté financière. Les relations presse et les relations publiques doivent porter sur l'image de compétence de l'établissement qui demeure identique à la compétence reconnue de la banque avant divulgation de la fraude. Les autorités de tutelle, les actionnaires, les clients, mais également les collaborateurs actuels et futurs de la banque doivent être les cibles privilégiées des campagnes de communication. Celles-ci doivent essentiellement permettre de répondre aux questions suivantes :

- ✓ Comment normaliser les relations avec les autorités de tutelle ? Comment obtenir un agrément dans un contexte si défavorable ? Comment enrayer toute suspicion de nouvelle fraude ?
- ✓ Comment les clients vont-ils réagir ?
- ✓ Comment vont réagir les actionnaires devant la perte qu'ils vont subir ?
- ✓ Comment annihiler tout impact sur les recrutements, les meilleurs profils seront-ils tout de même attirés ? Comment maintenir le sentiment de fierté d'appartenance des collaborateurs ?

© IFACI

1.2.3 - Quelques exemples d'impact de fraude

Les cas de fraude les plus célèbres de l'histoire financière récente concernent la **banque d'investissement** et leur impact sur les comptes, où même la survie des établissements qui en ont été les victimes, a été considérable.

Ainsi la banque Barings, un des plus anciens et prestigieux établissements de la City, a disparu, cédée pour une livre symbolique à ING, après la découverte en septembre 1995 de la perte due aux agissements de Nick Leeson. Ce dernier, basé à Singapour, arbitrait les marchés actions. Ses revenus enregistrés contribuaient à 10% des profits globaux de Barings. En fait, Nick Leeson dissimulait ses pertes dans un compte d'erreur que son passé d'opérateur back-office lui avait permis d'ouvrir et de dissimuler pendant trois ans. Pour tenter de résorber ses pertes initiales il avait eu recours à des stratégies de plus en plus risquées, ne parvenant qu'à les creuser d'avantage, jusqu'à hauteur de 827 M£ lorsque l'affaire fut découverte.

Plus sophistiquée fut la fraude de Toshihide Iguchi, trader sur bonds chez Daïwa, qui mit aussi son expérience d'opérateur back-office pour établir pendant 11 ans de faux avis d'opéré (30 000) et dissimuler ainsi ses pertes. Teshihide Iguchi, dépassé par l'ampleur de sa fraude, avait fini par se dénoncer lui même à ses supérieurs. Daïwa fut condamné par les autorités américaines et amené à renoncer à sa licence d'opérer aux Etats-Unis.

Sur une classe de produits différents, les matières premières, un autre établissement japonais devait connaître peu de temps après une certaine célébrité. Yasuo Hamanaka intervenait pour le compte de Sumitomo Corporation sur le marché du cuivre. Ses positions très importantes l'ont conduit à manipuler le marché ou, du moins, à tenter de le faire, mais au risque de prendre des positions qui finalement se sont avérées perdantes dans des proportions considérables, avec un impact non seulement sur Sumitomo Corporation, mais aussi sur le marché même du cuivre.

Bien entendu, on ne saurait oublier la fraude au sein de la Société Générale en 2008, même si l'affaire n'ayant pas encore été jugée, il n'en sera fait que mention à ce stade.

Dans le domaine de la **banque privée**, la personnalisation extrême de la relation entre un client, ou un groupe de clients, et un collaborateur de l'établissement est un facteur favorisant la fraude interne. Lorsque cette situation se double d'une reddition de comptes faite non pas de manière automatique mais grâce à des états manuels élaborés par le collaborateur en charge de la relation, la situation est potentiellement dangereuse. Le cas des clients optant pour le service de « courrier confié », et ainsi susceptibles d'être victimes de fraude, est fréquent.

Un cas exemplaire datant de 2001 est celui d'un gérant de fortune de Deutsche Bank USA : aucun courrier n'était envoyé aux clients et les contacts avaient lieu au cours de rendez-vous semestriels, éventuellement complétés d'entretiens téléphoniques. Le gérant présentait la situation des comptes et des avoirs à partir de documents personnalisés qu'il élaborait lui-même. Suite à l'ab-

© IFACI

sence du gérant au moment d'une demande de transfert, le caractère fictif des situations présentées par celui-ci a été révélé.

En décembre 2008, une escroquerie de type pyramide de Ponzi a entraîné des pertes estimées à environ 50 milliards de dollars. La société d'investissement de Bernard Madoff payait les intérêts des premiers investisseurs avec le capital apporté par les derniers entrés. La crise financière ayant incité certains clients à retirer leurs fonds, la pyramide s'est écroulée avec un fort retentissement au niveau international.

Pour être moins significatives en termes de montants, mais aussi plus nombreuses, les fraudes dans les autres compartiments de la banque n'en ont pas moins des conséquences très négatives, en termes d'image, d'incidence sur le fonctionnement des services concernés aussi. Bien souvent la découverte de la fraude constitue un véritable traumatisme pour les équipes confrontées à ces événements et, si cet aspect est difficile à mesurer, il ne doit certainement pas être sous-estimé.
Dans la **banque de détail**, les cas les plus nombreux sont les suivants:

- vol d'espèces ;
- fausses factures de fournisseurs ;
- prélèvement frauduleux sur des comptes internes (notamment comptes de passage, comptes de régularisation, etc.) et des comptes de particuliers (personnes âgées, sans mouvement ou au contraire volumes d'écritures importants, etc.) ;
- fraudes au crédit (dossiers fictifs, prorogations d'échéances, dépassements de crédit, etc.) ;
- transferts de fonds suivis de découvert et/ou fermeture de compte, avec complicité externe.

1.3- Typologie de la fraude

Il convient de distinguer deux grandes catégories de fraude : la fraude interne et la fraude externe[1].

- La **fraude interne**, commise par un collaborateur, est une faute professionnelle. Elle peut être sanctionnée sur le plan disciplinaire, sans préjudice des éventuelles poursuites et sanctions administratives, civiles et pénales.
  Le cas échéant, elle peut être commise sous le couvert d'un proche qui a, avec le collaborateur, soit des liens familiaux (son conjoint, les enfants sur lesquels il exerce l'autorité parentale ou dont il a la charge, ou toute autre personne à sa charge ou résidant à son domicile par exemple), soit des liens étroits (une personne morale par exemple dont le collaborateur

[1] *L'annexe IV de l'arrêté du 20 février 2007 donne une classification des types de perte opérationnelle parmi lesquelles : la **fraude interne** : « Pertes liées à des actes commis à l'intérieur d'une entreprise visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou règlementaire, ou des règles de l'entreprise, à l'exclusion des cas de pratiques discriminatoires ou contraires aux règles en matière d'égalité professionnelle, et impliquant au moins un membre de l'entreprise ». Et la **fraude externe** : « Pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou règlementaire ».*

© IFACI

et/ou ses proches détiennent directement ou indirectement une part du capital, des droits de vote ou des intérêts économiques).

La fraude commise en dehors des activités professionnelles du collaborateur doit être considérée comme une « fraude interne » s'il en résulte un trouble caractérisé dans le fonctionnement de la banque et, éventuellement, sa mise en cause par les personnes lésées. Il en est ainsi, notamment, de la pratique d'opérations qui peuvent s'apparenter à des opérations de banque (recel de fonds, avances de trésorerie, etc.) mais qui ne sont ni conduites dans le cadre de l'établissement pour lequel travaille l'individu concerné, ni régulièrement enregistrées dans ses comptes. Relève également de cette catégorie la communication à des tiers d'informations internes confidentielles (numéros de comptes, de cartes de crédit, etc.) permettant d'effectuer des opérations frauduleuses.

De même, la corruption active[1] telle que définie par l'article 445-1 du Code Pénal et la corruption passive définie à l'article 445-2 du Code pénal sont constitutives d'une fraude interne.

- La **fraude externe** est perpétrée par un tiers. La banque pourrait être (ou est) la victime directe (par exemple, lorsqu'il y a un vol d'actif ou de données, un piratage) ou la victime indirecte (par exemple, une fraude portant sur des actifs dont la banque a la garde ou portant atteinte à sa réputation sans qu'elle en soit la victime directe).

[1] *Fiche pratique sur la corruption privée, Rapport de 2005 du Service central de la prévention de la corruption, chap.5 p.223 ou www.justice.gouv.fr*

© IFACI

1.3.1 – Principaux types de fraude

Dans les paragraphes suivants, le groupe de travail propose une typologie des cas de fraude dans les établissements financiers et commente le profil des fraudeurs.

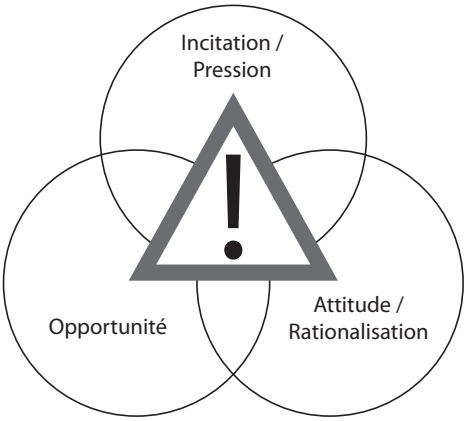
Les exemples de fraude dans les établissements financiers peuvent être classés selon cinq catégories d'actes de malveillance :

I	**Détournement de fonds direct** (manipulation des comptes, des avoirs)	1. Détournement sur fonds propres de la banque (y compris les actifs physiques) ; 2. Détournement sur comptes de clientèle.
II	**Détournement de fonds indirect** (manipulation des outils de gestion, des processus)	1. Remboursement de frais indus, auto-attribution de commissions indues ; 2. Décaissement de crédits fictifs, crédits de complaisance ; 3. Corruption (dans les appels d'offre, lors de la revente d'actifs financés saisis par la banque).
III	**Atteintes à la sécurité informatique**	1. Dommages dus au piratage informatique ; 2. Détournement des outils informatiques à des fins frauduleuses (manipulation des outils de paye, etc.) ; 3. Vol d'informations stockées sur des supports informatiques.
IV	**Divers manquements déontologiques préjudiciables pour la banque** (préjudice financier ou d'image)	1. Blanchiment d'argent (ou facilitation de) ; 2. Abus de marché : délit d'initié et manipulations de marché ; 3. Falsification de chèques, contrefaçon de carte bancaire, cavalerie (ou facilitation de) ; 4. Utilisation impropre d'informations privilégiées ou sensibles ; 5. Corruption ; 6. Abus de confiance.
V	**Autres activités non autorisées ou dissimulées**	1. En l'absence d'autorisation, prise d'engagement (activités de crédits) ou de positions sur les marchés financiers (« rogue trading ») ; 2. Dissimulation d'engagements compromis / de pertes ; 3. Falsification de l'information financière dans les comptes consolidés.

© IFACI

1.3.2 - Le triangle de la fraude

L'approche de Donald Cressey, plus connue sous la représentation d'un « triangle de la fraude », constitue un cadre conceptuel permettant de comprendre la fraude. Il est important de sensibiliser le management à ces différents critères.
Il se compose de trois éléments : la perception d'incitations/de pressions, la perception d'opportunités et la justification rationnelle du comportement frauduleux.



Incitation/Pression – L'employé rencontre des difficultés financières ou il subit une pression (objectifs commerciaux, système de rémunération variable inadapté, etc.) de la part de son management.

Opportunité – L'absence de contrôles, l'inefficacité des contrôles en place, la confiance aveugle accordée à un employé… donnent l'opportunité de commettre une fraude.

Rationalisation – C'est la justification morale et rationnelle de l'acte de fraude, ce qui constitue un mécanisme psychologique permettant de faire face à l'inévitable « dissonance cognitive » (c'est-à-dire la tension entre l'impression d'être honnête et la nature frauduleuse des actes).

Des statistiques confirment cette analyse :

- l'auteur de la fraude a besoin de maintenir un train de vie élevé (39%) - une incitation / pression ;
- le dispositif de contrôle interne de l'entreprise présente des faiblesses (41%) – une opportunité ;
- la faible prise de conscience que l'auteur commettait une fraude (52%) – un moyen (inconscient) de rationalisation.

1.3.3 - Profil du fraudeur

Le fraudeur peut être n'importe qui et le fraudeur le plus dangereux est certainement « Monsieur tout le monde », le collègue ou le conseiller que rien ne laisse soupçonner, à l'instar de Bernard Madoff ou d'autres fraudeurs mentionnés précédemment.

La motivation est le plus souvent financière. Elle recouvre des comportements différents qui vont de la situation du caissier qui « emprunte » une somme dans la caisse dont il a la responsabilité au « rogue trader » qui dissimule une position perdante, en passant par l'assistante ou le manager

© IFACI

qui falsifie des demandes de remboursement de frais professionnels. Tous ces cas ont un point commun, la dissimulation qui suppose un certain entregent, ce qui permet au fraudeur de confondre ses supérieurs et d'échapper aux contrôles.

Dans la quatrième édition de l'enquête sur la fraude dans les entreprises en France, en Europe et dans le monde réalisée par PricewaterhouseCoopers en 2008, une section spécifique est dédiée au profil du fraudeur :

- Lorsque l'on considère les cas de fraude les plus sérieux, on constate qu'environ une fois sur deux il s'agit d'un salarié de l'entreprise (46% en France) et le reste du temps un tiers sans lien particulier avec l'entreprise (32% en France), soit encore un client ou un fournisseur.
- Le fraudeur interne est généralement un homme (dans 93% des cas), âgé en moyenne de 40 ans qui occupe dans près de 55% des cas une position élevée dans la hiérarchie (top management dans 29% des cas ou middle management dans 26 % des cas). Il travaille dans l'entreprise depuis 9 ans, mais dans 20% des cas, il est arrivé dans l'entreprise au cours des deux dernières années.
- Il est plutôt sympathique et apprécié par sa hiérarchie, il semble souvent surchargé, voire mal organisé dans son travail et il part peu en vacances, par conséquent il ne partage pas ses dossiers.
- La motivation (généralement financière) et la capacité d'autojustification jouent un rôle prépondérant dans la décision du fraudeur de passer à l'acte. Or, les procédures et les contrôles mis en place ne vont pas nécessairement le gêner puisqu'il en a une connaissance parfaite. Le fraudeur sait gérer la fraude à long terme.

Aucune statistique ou étude spécifique n'a, à ce jour, été réalisée sur l'incidence de la forte mobilité interne ou de la complexité des contrôles et des produits dans les établissements financiers, mais il s'agit de facteurs à suivre dans l'avenir.

Un rapport annuel de l'ACFE vient compléter ces statistiques notamment dans les domaines suivants (cf. annexe 2, p. 86) :

L'âge des fraudeurs : Le rapport entre l'âge du fraudeur et le montant des pertes moyennes est fort. Toutefois, il est important de noter la corrélation naturelle entre l'âge et la place occupée par l'auteur de fraude et son ancienneté dans l'entreprise.

L'ancienneté des fraudeurs : on peut noter une corrélation directe entre l'ancienneté et les pertes moyennes. L'enquête de l'ACFE montre ainsi que plus un salarié est ancien :

- plus il a de possibilités de monter en hiérarchie ;
- plus il connaît les contrôles à déjouer ;
- plus il a la confiance de ses supérieurs et collègues.

Les études statistiques permettent de définir a posteriori un profil type. Toutefois, il serait assez hasardeux de baser des contrôles uniquement à partir de ces données. Par ailleurs, on peut noter que 87% des cas de fraude on été perpétrés par des individus avec un casier judiciaire vierge.

© IFACI

D'après plusieurs études dans le contexte de la crise économique et financière, le nombre de fraudes ainsi que leur gravité ont sensiblement augmenté en 2008.
Parmi les types de fraudes, le vol, la corruption et le délit d'initié ont enregistré les plus fortes progressions dans tous les pays.

© IFACI

Partie II

Audit interne et risque de fraude : la position de l'IIA et des principaux régulateurs

Après avoir dressé la cartographie de la fraude, le présent chapitre a pour objet d'indiquer la position de l'IIA et des principaux régulateurs, positions qui constituent le cadre directeur des interventions de l'audit.

© IFACI

© IFACI

2.1 – Position de l'Institute of Internal Auditors (IIA)

La lutte contre la fraude s'insère à la fois dans les processus de gouvernement d'entreprise, de gestion des risques et de contrôle. Ce lien avec les trois processus-clés de la définition internationale de l'audit interne fait du dispositif de lutte contre la fraude un sujet d'audit par excellence. L'évolution récente du cadre de référence international des pratiques professionnelles (CRIPP[1]) précise les responsabilités de l'audit interne dans ces différents domaines ainsi que la prise en compte de la fraude dans la gestion du service d'audit interne.

Parmi les éléments dont le responsable de l'audit interne doit rendre compte périodiquement à la direction générale et au Conseil, la Norme 2060 met particulièrement en exergue une information sur l'exposition aux risques significatifs (y compris les risques de fraude) et les contrôles correspondants. Pour ce faire, le responsable de l'audit interne aura préalablement pris soin de définir les attentes des organes de gouvernance sur cette problématique et d'établir les responsabilités de son service en la matière. En effet, comme indiqué dans la Modalité Pratique d'Application (MPA) 2120-2 publiée en avril 2009, c'est souvent au moment de la découverte d'une fraude que se pose la question « où sont les auditeurs ? ». Pour assurer la gestion du risque dans le service d'audit interne, il s'agit de s'interroger notamment sur son mandat et ses moyens d'action pour :

- soutenir les efforts du management dans l'établissement d'une culture d'éthique et d'intégrité ;
- évaluer l'efficacité des processus de management des risques de fraude et contribuer à leur amélioration ;
- évaluer les dispositifs de contrôle interne mis en place par le management pour comprendre les indicateurs de fraude, prévenir et détecter les fraudes.

L'exercice de ces responsabilités doit être précisé au niveau de la gestion du service et à chaque stade du processus de lutte anti-fraude.

[1] *Le cadre de référence international des pratiques professionnelles sont disponibles sur le site de l'IFACI (www.ifaci.com)*

© IFACI

Les responsabilités de l'audit interne pour chaque volet de la lutte anti-fraude

Volet du dispositif de lutte anti-fraude	Responsabilités de l'audit interne
Programme de gestion du risque de fraude au niveau de l'organisation	✓ Est-il **formalisé** ? Si non, les organes de gouvernance sont-ils informés des avantages de la mise en place d'un tel programme ? ✓ Traduit-il, soutient-il les attentes des organes dirigeants ? ✓ Comment l'exposition au **risque de fraude** est prise en compte ? - benchmark sur la probabilité d'occurrence et les conséquences de la fraude , - vigilance sur l'actualisation du niveau d'exposition, - évaluation de la qualité des dispositifs de maîtrise de risque, - couverture suffisante du périmètre de l'organisation y compris les relations avec les sous-traitants, - exhaustivité du spectre d'impact qui ne doit pas uniquement se limiter au seul aspect financier mais prendre en compte d'autres aspects comme le risque d'image, de continuité, etc.) ✓ Les **moyens** nécessaires à la mise en œuvre de ce programme sont-ils adéquats et suffisants ? - ressources humaines localisées ou non au sein de l'audit interne, - relais dans les entités opérationnelles, - capacité de l'organisation à gérer de manière diligente le risque de fraude, - reporting anonyme, - outils informatiques et de communication, etc. ✓ Approche coordonnée des **actions correctives** : tirer les leçons de l'expérience et les diffuser au niveau le plus approprié de l'organisation.
Prévention	• Impact des objectifs et indicateurs de performance sur l'environnement de contrôle (ex : politique de rémunération). • Connaissance des meilleures pratiques et mise en œuvre de techniques de prévention. • Programme support de sensibilisation des salariés avec des actions spécifiques pour les managers - qu'attend-on des salariés ? - comment se traduisent les notions d'intégrité et d'exemplarité ? - quels sont les points de vigilance en matière de gestion des ressources humaines ? • Qualité et sécurité du processus de reporting des soupçons de fraude.

© IFACI

Volet du dispositif de lutte anti-fraude	Responsabilités de l'audit interne
Détection	• Connaissance des meilleures pratiques et mise en œuvre de techniques de détection. • Compréhension et analyse des indicateurs de fraude. • Evaluation du risque financier, opérationnel, de réputation. • Evaluation du dispositif de contrôle interne mis en place par le management pour prévenir, détecter et maîtriser les risques de fraude. • Analyse décisionnelle des systèmes d'information.
Investigation	• Compétences et niveau de reporting adéquats de l'équipe d'investigation. • Mesure coûts/bénéfices des actions correctives.

Sans être des experts en détection de la fraude, les auditeurs internes doivent évaluer la pertinence, l'efficacité et l'efficience des mesures de lutte contre la fraude.
Ces responsabilités doivent être inscrites dans la charte d'audit interne et être intégrées dans le plan d'audit et à chaque stade de l'activité du service.

2.2 – Rappel du cadre réglementaire

En ce qui concerne la prévention de la fraude dans les établissements financiers, deux types d'approche sont adoptées selon les pays. En France et au Royaume Uni, le sujet relève désormais de dispositions spécifiques qui sont détaillées ci-après. En revanche, dans d'autres pays tels que les Etats-Unis ou les Pays-Bas, les autorités de surveillance intègrent lors de leurs contrôles le risque de fraude interne ; ce risque est simplement considéré comme faisant partie du risque opérationnel au sens large (cf. annexe 3, p.87).

2.2.1 – France

La lutte anti-fraude s'articule autour de trois principaux textes :

- Le rapport de Christine LAGARDE au Premier Ministre concernant les enseignements à tirer des évènements intervenus à la Société Générale (2008).
- Le règlement CRBF 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédits et des entreprises d'investissement modifié en particulier par arrêté du 14 janvier 2009, publié le 30 janvier 2009.
- La réglementation Bâle II.

© IFACI

1 - **Les recommandations du rapport Lagarde** visent à renforcer les dispositifs internes de contrôle des établissements exerçant des activités de marchés au travers des points de contrôle suivants :

- surveillance des encours nominaux des opérateurs (par opposition à la surveillance des positions nettes qui ne fait par définition apparaître qu'un risque de marché limité) ;
- suivi des flux de trésorerie (appels et versement de marge, dépôts de garantie, résultats réalisés) ;
- exploitation approfondie des demandes d'information de la part d'entreprises de marché ;
- suivi des annulations et modifications de transactions provenant d'un seul opérateur et piste d'audit garantie pour chaque transaction de chaque opérateur ;
- réconciliation des confirmations des opérations avec l'ensemble des contreparties (y compris avec les contreparties internes à un groupe). Documentation précise des termes et conditions des opérations nouées avec les contreparties externes. Attention renforcée dans le domaine des dérivés, en particulier s'agissant des conditions contractuelles, en recourant autant que possible aux contrats-type élaborés par les associations professionnelles ;
- respect de l'indépendance entre le front-office et le back-office et transversalité de l'organisation du middle-office et du back-office ;
- sécurité des systèmes d'information et protection des codes d'accès ;
- surveillance des comportements atypiques (absence de congés par exemple). Organisation des dispositifs de contrôle au niveau des salles de marché qui permette un suivi global des transactions de chaque opérateur, de façon à pouvoir déterminer son profil d'activité et donc identifier plus aisément des comportements inhabituels ;
- conformité des engagements des opérateurs au regard de leur mandat : des termes écrits devraient systématiquement définir précisément les opérations permises à chaque opérateur. Ils permettraient de s'assurer que la nature et le montant des instruments financiers utilisés s'inscrivent bien à l'intérieur des limites fixées et de la stratégie définie par l'établissement.

2 - **Les dispositions du règlement CRBF 97-02 modifié,** texte fondamental en termes de contrôle interne bancaire, intègrent le risque de fraude. Ce texte précise, en particulier, dans son article 4-j que « *le risque opérationnel inclut les risques de fraude interne et externe tels que définis à l'annexe IV de l'arrêté du 20 février 2007* ». En outre, les systèmes de mesure et d'analyse des risques doivent appréhender le risque opérationnel (article 17).

Plus globalement, ce risque est pris en compte par ce règlement, à l'instar de tous les autres risques auxquels la banque est exposée. A titre d'exemple, les objectifs assignés au dispositif de contrôle interne en matière de contrôle des opérations et des procédures internes (article 5) sont de :

- « *vérifier que les opérations réalisées [...] sont conformes [...]* » et ainsi, de prévenir et détecter les opérations irrégulières et frauduleuses ;
- « *vérifier que les procédures de décision, de prises de risques, sont strictement respectées* » et ainsi de limiter le risque de fraude en précisant les personnes habilitées à décider ou fixer des limites ;

© IFACI

- « *vérifier la qualité de l'information comptable et financière [...]* » et d'éviter la présentation volontaire de bilan ou de données internes inexacts ;
- « *vérifier les conditions d'évaluation, d'enregistrement, de conservation [...]* » et ainsi de limiter, par le respect de la piste d'audit, l'introduction de données fictives, ainsi que la modification ou l'annulation frauduleuse de données ;
- « *vérifier la qualité des systèmes d'information et de communication [...]* » et donc de s'assurer de l'existence de systèmes d'information sécurisés.

De plus, les moyens préconisés par le règlement CRBF 97-02, avec un double dispositif de contrôle permanent et périodique adapté aux activités, à la taille et aux implantations et un principe de séparation des tâches, doivent contribuer à limiter le risque de fraude.

L'article 17-ter précise également que « *les systèmes d'analyse et de mesure des risques prévus à l'article 17 doivent prévoir les critères et seuils permettant d'identifier comme significatifs les incidents révélés par les procédures de contrôle interne au sens de l'article L. 511-41 du Code Monétaire et Financier. Ces critères doivent être adaptés à l'activité de l'établissement et couvrir les risques de perte, y compris lorsque celle-ci ne s'est pas matérialisée.*
Est réputée significative toute fraude entraînant une perte ou un gain d'un montant brut dépassant 0,5% des fonds propres de base. Ce montant ne peut être inférieur à dix mille euros ».
L'organe délibérant doit par ailleurs arrêter les critères et seuils de significativité mentionnés à l'article 17 ter du règlement CRBF 97-02 permettant d'identifier les incidents devant être portés à sa connaissance.
Les responsabilités de l'organe exécutif sont sur ce point :

- de les faire parvenir à la Commission bancaire qui vérifiera leur pertinence (et peut lui demander de revoir ces critères et seuils ainsi que les modalités de leur mise en œuvre) ;
- et de lui transmettre sans délai les incidents significatifs.

3 - <u>Le Comité de Bâle</u>, dans son document sur les « Principes fondamentaux pour un contrôle bancaire efficace »[1], a pris position quant à la question de la fraude dans son principe 15 qui précise :
« *Il s'agit notamment de prévenir et de repérer les actes délictueux ou frauduleux et d'informer les autorités compétentes des faits soupçonnés. […] En plus d'informer les autorités judiciaires compétentes, les banques signalent à l'autorité de contrôle les activités litigieuses et tout cas important de fraude vis-à-vis de la sécurité, de la solidité ou de la réputation de la banque.* »

Le Comité de Bâle a identifié la complexité croissante des opérations bancaires comme une source significative de risque de fraude et a replacé la question de la fraude en milieu bancaire au premier plan des préoccupations des banques, en nommant explicitement la fraude comme composante du risque opérationnel.

[1] *Note méthodologique d'octobre 1999.*

© IFACI

L'accord de Bâle II définit le risque opérationnel comme le « *risque de pertes résultant de carences ou de défaillances attribuables à des procédures, des personnes et systèmes internes ou à des événements extérieurs* ». Les fraudes externes et internes sont ainsi identifiées dans les sept catégories d'événements des risques opérationnels.

L'application de ces dispositions doit permettre aux établissements de se prémunir contre le risque de fraude. Ces derniers doivent identifier, évaluer et suivre le risque de fraude afin de proposer l'affectation d'une partie de leurs fonds propres à la couverture de ce risque.

2.2.2 - Royaume-Uni

En 2006, la FSA[1] a publié le « Fraud Act », texte officiellement entré en vigueur, après consultation des parties intéressées, le 15 janvier 2007. Les éléments relatifs à la fraude, précédemment inscrits au sein du « Prudential Sourcebook » sont, depuis janvier 2007, refondus dans la section SYSC du « FSA Handbook » relative aux systèmes et contrôles des risques. La fraude est assimilée au risque opérationnel (§13.5).

Les dispositions principales du « Fraud Act » sont les suivantes :

1 - Une **définition** qui insiste sur le « modus operandi » comme élément déterminant dans la qualification des faits. Une fraude est commise par représentation mensongère (« false representation »), dissimulation et manipulation d'information(s) ou encore détournement de fonction (« abuse of position »). Le fait d'obtenir un avantage indu par déloyauté ou toute manœuvre malhonnête est également constitutif d'une fraude.

2 - La FSA n'a pas défini un **dispositif** précis à appliquer pour prévenir la fraude, comme par exemple en matière de lutte anti-blanchiment, mais il est demandé aux établissements de prendre toutes les dispositions nécessaires pour parer à ce risque.
Le « FSA Handbook » exige des établissements assujettis qu'ils soient en mesure de mettre en place des processus permettant d'identifier, de gérer, de suivre et de rapporter les risques auxquels ils font, ou pourraient faire face : *"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime".*

3 - La FSA souligne que l'**environnement** actuel est générateur de risques de fraude, notamment pour les raisons suivantes :

[1] *FSA : Financial Services Authority*

© IFACI

- la sophistication croissante des techniques bancaires, les produits complexes, les communications électroniques ;
- un personnel trop souvent soumis à de fortes pressions pour atteindre les objectifs et parfois déstabilisé par des menaces de licenciement ou encore l'absence de visibilité sur leur devenir.

4 - Des obligations de **reporting** très étendues. La banque doit notifier immédiatement toute fraude de montant significatif, les erreurs et autres irrégularités, particulièrement quand un client est concerné. La déclaration doit préciser la victime, qu'il s'agisse directement de la banque ou d'une de ses relations commerciales. Le soupçon de fraude doit aussi être déclaré aux autorités.
La FSA souligne que l'information du régulateur a non seulement pour objet de l'informer sur la nature des irrégularités commises, mais aussi de protéger les clients ou les autres établissements qui pourraient être éventuellement touchés. De plus, la FSA doit être en mesure d'apprécier rapidement, d'une part l'impact de la fraude sur les comptes et la réputation de l'établissement concerné, d'autre part d'évaluer si cet événement révèle des défaillances dans l'organisation et le système de contrôle.

5 - Des **sanctions** : La sanction pénale la plus élevée pour un employé de banque coupable de fraude est une peine de 10 années d'emprisonnement. Elle est au maximum de 5 ans pour un employé qui n'a pas signalé une fraude et de deux ans pour celui qui a prévenu un suspect qu'une enquête était en cours (« tipping off »).
Par ailleurs, des amendes peuvent être infligées aux établissements qui n'auraient pas pris les mesures adéquates pour lutter contre le risque de fraude. Depuis quelques années, plusieurs établissements ont été pénalisés pour des montants significatifs[1].

6 - Des revues périodiques : Lors de ses revues d'activités périodiques (« Arrow Review »), la FSA consacre des entretiens et des moyens spécifiques et tout à fait conséquents, au sujet de la fraude.

[1] *En 2008, la FSA infligé une amende (5 600 000£) à un établissement assujetti pour non-respect du 3ème principe, entre autre, des « FSA's Principles for Business », selon lequel tout établissement doit veiller à l'efficacité de ses systèmes et de ses contrôles en matière de risque de fraude.*

© IFACI

© IFACI

Partie III

Gouvernance et pilotage du dispositif de lutte contre la fraude

© IFACI

© IFACI

3.1 – Les acteurs clés du dispositif

Compte tenu des risques encourus par les organisations comme de la nature même du sujet, la fraude est un sujet de gouvernance globale. Comme tel, il concerne l'ensemble des acteurs de l'organisation, en commençant par une implication des organes dirigeants au plus haut niveau, Conseil d'administration, éclairé par le comité d'audit, direction générale et comité exécutif ainsi que l'ensemble des opérationnels et du dispositif de contrôle permanent.

Le Conseil d'administration représente collectivement les actionnaires. Il contrôle la gestion et veille à la qualité de l'information qui leur est fournie. Au-delà de l'impératif moral, le Conseil est donc garant de la confiance que placent les différents acteurs économiques dans la banque et garant de son bon fonctionnement. A ce titre, la fraude et plus largement les questions d'éthique sont donc des sujets qui le concernent au premier chef.

Le rôle du comité d'audit est de s'assurer, par des entretiens réguliers avec le responsable de l'audit interne mais aussi les commissaires aux comptes ou encore le directeur financier, le directeur des risques ou de la conformité, que des dispositifs sont mis en place pour parer au risque de fraude. Dans les établissements où une fraude majeure est survenue, le comité d'audit devra suivre la mise en place des mesures de remédiation, éventuellement en créant un comité spécial chargé de ce suivi.

Selon l'article 14 de l'ordonnance 8 décembre 2008 transposant la directive du 17 mai 2006 et relative aux commissaires aux comptes, « *Sans préjudice des compétences des organes chargés de l'administration, de la direction et de la surveillance, ce comité est notamment chargé d'assurer le suivi :*

a) Du processus d'élaboration de l'information financière ;
b) De l'efficacité des systèmes de contrôle interne et de gestion des risques ;
c) Du contrôle légal des comptes annuels et, le cas échéant, des comptes consolidés par les commissaires aux comptes ;
d) De l'indépendance des commissaires aux comptes. »

Le règlement bancaire 97-02 précise le devoir d'alerte du responsable de l'audit interne dans l'article 9-1 : « *Les entreprises assujetties définissent des procédures qui permettent : […] b) Au responsable du contrôle périodique d'informer directement et de sa propre initiative le comité d'audit de l'absence d'exécution des mesures correctrices décidées.* » De plus, le texte mentionne les conditions de mise en place des critères et seuils des systèmes d'analyse et de mesure des risques, système permettant d'identifier les incidents significatifs révélés par les procédures de contrôle interne.

© IFACI

Le directeur général, pour sa part, doit veiller à ce que les préoccupations de lutte contre la fraude soient bien prises en compte dans les plans d'audit qui lui sont soumis. Il doit aussi se tenir très régulièrement informé des fraudes décelées et des investigations menées à cette occasion, pour en tirer éventuellement toutes les leçons en termes de priorité et d'organisation générale. Enfin, et c'est sans doute le plus important, il doit s'assurer que dans le mandat de chaque responsable de pôle, membre du comité exécutif, il est bien fait référence à des mesures traduisant une attitude de vigilance active à l'égard de la fraude.
De même, chaque membre du comité exécutif devra « cascader » ces mesures sur ses adjoints. Cette référence est reprise dans le cadre de leurs mandats et de leurs objectifs annuels, en fonction de leurs périmètres de compétence.
De surcroît, et pour leur permettre de remplir efficacement leur mission, il paraît hautement souhaitable d'organiser pour les managers et leurs équipes des formations et des séances de sensibilisation au risque de fraude, sachant que c'est, en premier lieu, au niveau du manager opérationnel que se jouent la réussite ou l'échec des dispositifs de prévention de la fraude.

Enfin, il convient de citer les dispositifs de rémunération qui ne doivent pas constituer pour tous les acteurs concernés des incitations, au moins indirectes, à la fraude. Le régulateur insiste aujourd'hui sur cet élément qui concerne tous les acteurs clés dans chaque organisation.

3.2 – Le mandat et le rôle de l'audit dans le dispositif de lutte contre la fraude

Le mandat de l'audit interne est défini par les directives internes de chaque établissement. Ces directives intègrent les principes de base en matière de contrôle interne au sein des banques et des institutions financières et incluent la gouvernance d'entreprise, la gestion des risques, l'adéquation et l'organisation du contrôle interne. Elles sont fondées sur les textes cités au chapitre II (cf. p. 28 et p.30) :

- le CRBF 97-02 pour la France ;
- les recommandations du comité Bâle d'Août 2001 ;
- ou encore le « Financial Security Act » d'Août 2003.

En matière de fraude, sujet particulièrement sensible, le mandat de l'audit interne doit être clairement établi. L'audit interne, **organe de contrôle périodique**, n'a pas de responsabilité de premier niveau. Celle-ci repose d'abord sur les managers et opérationnels en charge directement des activités. L'audit interne n'a pas non plus d'obligation de résultat, c'est-à-dire d'obligation de déceler tous les cas de fraude.

En revanche, l'audit interne doit intégrer de manière très explicite le risque de fraude dans la procédure de « risk assessment » et être en mesure de justifier les conclusions de la procédure de ce point de vue. Ensuite, l'audit interne doit assurer de manière systématique des contrôles « anti-

© IFACI

fraude » dans le cadre des vérifications courantes, notamment sur les activités ou les procédures considérées comme particulièrement risquées. Enfin, l'audit interne doit alerter rapidement sur les dysfonctionnements susceptibles de favoriser la fraude et suivre activement la mise en place des recommandations. Il doit également assurer une remontée de l'information sur les retards éventuels dans la mise en œuvre de ces recommandations.

En tout état de cause, l'audit interne peut effectuer des vérifications ciblées, courtes et inopinées sur des problématiques de sécurité, hors plan d'audit, généraliser l'utilisation d'extracteurs de données pour « attaquer » les fichiers complexes et volumineux, enfin systématiser les approches intégrées audit métiers/audit des systèmes d'information.

Pour les missions liées à la fraude, deux conditions principales doivent être remplies. En premier lieu, et c'est un aspect tout à fait critique, le rattachement à la direction générale, les liens avec le comité d'audit ou bien encore la coordination avec les commissaires aux comptes doivent assurer l'indépendance nécessaire à des interventions portant sur des cas de fraude mettant en cause soit l'organisation générale d'un département, soit le « Top Management » de la banque. En second lieu, le service d'audit interne doit disposer des ressources nécessaires, tant en nombre d'agents que de niveau d'expertise de ceux-ci, et éventuellement disposer aussi des outils informatiques permettant les investigations.

Le responsable de l'audit interne doit intégrer, de manière transversale, le risque de fraude dans la gestion de ses ressources et des méthodes utilisées dans son service. Cette responsabilité incombe également individuellement à chaque auditeur interne.
En appliquant la Norme 2030, le responsable de l'audit interne doit évaluer les compétences de son service. La MPA 2030-1 précise que cette évaluation porte notamment sur les compétences de gestion, de prévention et de détection des fraudes. De même, la MPA 1210-1 cite, parmi les compétences nécessaires à l'exercice des responsabilités de l'audit interne :

- la connaissance permettant d'identifier les risques de fraude ;
- la compréhension des notions fondamentales de la conduite des affaires telles le management des risques et la fraude. Cette compréhension permet de reconnaître l'existence ou l'éventualité de problèmes.

Au terme de l'évaluation des compétences individuelles et collectives de son service, le responsable de l'audit interne identifie les actions nécessaires pour combler les lacunes éventuelles :

- programme de formation ;
- coordination avec d'autres acteurs internes ;
- recrutement d'un expert ;
- recours à des prestataires externes. En effet, comme indiqué dans la MPA 1210.A1-1, l'audit interne peut faire appel à des prestataires externes notamment dans les cas d'enquêtes sur la fraude et la sécurité.

© IFACI

Le choix entre les différentes options dépendra de la capacité de développement des compétences existantes, de la nature des risques (par exemple, savoir-faire en informatique) et du rapport coût/bénéfice.

L'optimisation des ressources passe nécessairement par la mise en œuvre de la Norme 2050 relative à la coordination : « *Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations et coordonner les activités avec les autres prestataires internes et externes d'assurance et de conseil* ».
Pour avoir l'assurance d'une prise en compte du risque de fraude au sein du service, le responsable de l'audit interne l'intègre également au niveau :

- de la planification (Normes 2010, 2020 et série 2200). Il s'agit de la phase d'identification des risques à partir desquels le plan d'audit va être construit, de la communication (qui doit faire l'objet d'une attention particulière en cas de missions sur la fraude) du plan, de son approbation par les organes de gouvernance mais également de son actualisation en cours d'année pour prendre en considération de nouveaux risques. L'analyse des risques et l'évaluation des ressources nécessaires à l'accomplissement des objectifs d'audit doivent être réitérées au niveau de chaque mission (Normes de la série 2200 : planification de la mission, objectifs de la mission, évaluation des risques dans la planification de la mission, ressources affectées à la mission, programme de travail de la mission) ;
- des règles et procédures (Norme 2040 et série 2300). « *Le responsable de l'audit interne doit établir des règles et procédures fournissant un cadre à l'activité de l'audit interne* ». En ce qui concerne la fraude, la mise en œuvre de ces procédures sera utilement complétée par les exigences des Normes de la série 2300 sur l'accomplissement des missions (identification des informations, analyse et évaluation, documentation des informations, contrôle de l'accès aux dossiers d'audit, conservation des dossiers, supervision de la mission) ;
- de la communication (Norme 2060 et série 2400). L'exigence de la Norme 2060 relative à une communication globale et périodique avec les instances de gouvernance est sous-tendue par la maîtrise de la communication au niveau de chaque mission. Il convient alors d'appliquer les principes édictés par les Normes de la série 2400 sur le contenu et la qualité de la communication ainsi que la diffusion des résultats ;
- de la surveillance des plans d'actions (Normes 2500 et 2600). Conformément à la Norme 2500.A1 « *le responsable de l'audit interne doit mettre en place un processus de suivi permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire* ».

Tous ces principes sont déclinés dans la MPA 2120-2 relative à la gestion du risque lié à l'activité d'audit interne. Par exemple :

- l'absence d'un processus efficace d'évaluation des risques pour identifier les principaux domaines d'audit, risque d'entraîner un gaspillage de ressources et une perte de temps sur des missions d'audits peu pertinentes (pour les systèmes d'information voir notamment le GTAG 11 : « developping the IT audit plan ») ;

© IFACI

- une mauvaise conception de procédures d'audit interne peut entraîner une défaillance lors de l'évaluation des risques « réels » et des contrôles adéquats. (cf. le GTAG 13 : « Fraud Prevention and Detection in an Automated World ») ;
- une prise en compte insuffisante des dispositifs de contrôles existant dans l'organisation (cf. GTAG 3 – Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques) ;
- une supervision insuffisante et inadéquate des activités d'audit interne ;
- des décisions inappropriées face à un soupçon de fraude (« ce n'est probablement pas important » ou « nous n'avons pas le temps ni les ressources pour gérer ce problème ») ;
- absence de communication des soupçons aux personnes appropriées.

La gestion collective du risque de fraude, au niveau du service d'audit interne, ne doit pas faire oublier le rôle individuel de l'auditeur interne. Ainsi selon la MPA 1220-1 : *« 1. […]En agissant avec la conscience professionnelle qui se doit, les auditeurs internes seront attentifs aux risques de fraude, de fautes intentionnelles, […] ainsi qu'aux situations et activités où des irrégularités ont le plus de chance de se produire. Les auditeurs internes sont également concernés par la détection de contrôles inefficaces et font des recommandations visant à promouvoir le respect des procédures et pratiques acceptables. […] ».*

Les auditeurs internes doivent tester systématiquement un certain nombre d'indicateurs au cours de chaque mission. Plus généralement, ils s'appuient sur les exigences des Normes de la série 2100 pour soutenir, évaluer et développer les dispositifs de lutte contre la fraude mise en place par l'organisation.

Une mission d'investigation de fraude doit être menée par une personne ayant une expertise dans le domaine et dûment habilitée. Certains établissements financiers mettent donc en place des équipes dédiées à ce type de mission, ayant été formées aux techniques d'investigation. Cependant, il n'est pas anormal que les équipes en charge du contrôle de troisième niveau participent ou mènent des missions d'investigation.

© IFACI

Enquête – Dispositif anti-fraude au sein des banques « Equipes dédiées à la prévention et à la lutte contre la fraude ? »

Afin de compléter le cahier de recherche de l'IFACI sur « L'audit de la fraude dans le secteur bancaire et financier », une enquête a été réalisée sur les dispositifs anti-fraude mis en place dans les principaux établissements bancaires opérant en France.
Le questionnaire s'est organisé autour des six grands thèmes suivants :

- Existence ou non d'une ou plusieurs équipes dédiés à la lutte et à la prévention contre la fraude.
- Organisation et direction de l'équipe.
- Ordre de mission de l'équipe.
- Prévention contre la fraude (techniques de prévention, Whistleblowing).
- Techniques et programmes de détection et d'investigation.
- Logiciels utilisés.

Cette enquête réalisée auprès de cinq établissements permet de faire émerger un certain nombre d'enseignements sur les pratiques en matière de lutte anti-fraude.

Equipes spécifiquement dédiés à la prévention et la détection des fraudes

Tous les établissements répondant ont mis en place ou vont mettre en place une ou des équipes dédiées à la prévention, la détection et parfois même l'investigation de la fraude.
La tendance générale consiste à considérer le risque de fraude comme un risque à traiter spécifiquement avec une équipe dédiée.

Hétérogénéité des modèles d'organisation

En dépit d'une position quasi-commune sur la mise en place d'équipes dédiées au risque de fraude, nous constatons une hétérogénéité dans le positionnement, les missions et le modèle d'organisation de ces équipes anti-fraude.
Ces équipes diffèrent principalement sur les points suivants :

- **Le rattachement hiérarchique** diffère selon les établissements et est assez diversifié: Conformité (2 banques), Chief Administrative Officier (1 banque), Sécurité (1 banque), Direction des risques opérationnels (1 banque) avec parfois un double rattachement Métiers/Direction des risques opérationnels.
- Si la prévention et la détection de la fraude font partie intégrante de **la lettre de mission des équipes** de tous les établissements, le périmètre de responsabilité diffère en matière d'investigation. Tous les cas de figure sont rencontrés :
  - soit ce rôle est exclu de la lettre de mission et est confié à d'autres équipes (le contrôle périodique en général) ;

© IFACI

- soit la responsabilité de l'investigation va dépendre de l'ampleur de la fraude, les fraudes importantes étant confiées au contrôle périodique ;
- soit l'équipe anti-fraude est pleinement en charge des investigations.

- La question de **la centralisation/décentralisation des équipes** fait également apparaître des modèles différents selon les établissements :
  - une équipe centralisée au siège en charge de tous les métiers du Groupe ;
  - une équipe de coordination au siège en relation avec des équipes spécialisées dans chaque branche métier ;
  - uniquement des équipes spécialisées dans les branches métier « à risque » (banque de détail, banque de financement et d'investissement et crédit à la consomation par exemple).

Taille réduite des équipes avec des profils expérimentés

Les équipes dédiées (l'équipe centrale en charge de la coordination et/ou les équipes métiers) sont de petite taille (entre 3 et 4 personnes) mais sont constituées de personnels expérimentés ayant l'expérience de la fraude.
Le nombre total d'individus dédiés aux équipes anti-fraude dépend du mode d'organisation (équipe centrale/équipes métiers, équipe centrale uniquement, quelques équipes métiers uniquement).
Les recrues proviennent d'horizons divers (compétences audit interne, métiers, informatiques, etc.).

Positionnement par rapport au dispositif de contrôle interne

Les modalités des échanges entre les équipes anti-fraude et les autres équipes du contrôle interne dépendent du positionnement et du rattachement hiérarchique des équipes anti-fraude :

- dans le cas d'un rattachement des équipes anti-fraude à la conformité, l'intégration des équipes anti-fraude au dispositif général de contrôle interne est facilitée ;
- dans le cas d'un rattachement distinct, des contacts réguliers sont organisés entre les équipes avec parfois l'envoi systématique des rapports à la direction de la conformité.

Un établissement interrogé mentionne la possibilité de conflit de compétence sur la responsabilité de l'investigation en cas de fraude.

Prévention

Le consensus se fait entre tous les établissements pour mettre en avant le rôle de la prévention via des campagnes d'information et de formation. Les équipes anti-fraude mettent également en avant le rôle du changement culturel à l'égard de la fraude comme un des piliers de la réussite. Ces campagnes sont généralement pilotées au niveau du Groupe.

© IFACI

La communication externe sur les fraudes rencontrées fait l'objet de plus de retenue et n'est envisagée qu'au cas par cas. La communication interne concerne les sanctions déjà prises.

Techniques de détection

Les pratiques en matière de détection sont relativement similaires entre les établissements et reposent principalement sur un système de remontée d'information via des contrôles et un dispositif d'alerte.

Ce point souligne l'importance de l'implication des équipes anti-fraude dans la conception des contrôles (seul un établissement n'implique pas les équipes anti-fraude dans la conception des contrôles).

Le recours au data mining est assez répandu. Les établissement qui n'utilisent pas encore cette technique de détection envisagent de le faire avec des logiciels spécifiques. Il est à noter que toutes les équipes anti-fraude disposent d'accès, en lecture, aux applicatifs métiers pour mener leur mission.

Les contrôles inopinés sont également une technique employée mais là les modèles divergent sur les acteurs de ces contrôles. En général, ces contrôles sont menés par les équipes de contrôle périodique ou permanent sauf pour un établissement pour lequel les équipes anti-fraude peuvent également mener leurs propres contrôles inopinés.

Whistleblowing

Tous les établissements interviewés ont mis en place un dispositif de Whistleblowing permettant de remonter les alertes levées par les salariés.

C'est un point important dans le dispositif anti-fraude dans la mesure où les salariés sont la première source de détection de la fraude : 36% en 2007 en France (« Enquête sur la fraude dans les entreprises en France, en Europe et dans le monde » Edition 2007, PwC).

Néanmoins, les liens entre ce dispositif et les équipes anti-fraude restent à renforcer (dans certains cas, le dispositif de Whistleblowing est géré par une autre équipe que l'équipe anti-fraude).

Comité nouveaux produits

Les réponses sont assez divergentes sur ce point et couvrent tout l'éventail des configurations possibles concernant l'implication des équipes anti-fraude dans ces comités nouveaux produits :

- systématiquement impliqué ;
- implication ponctuelle au besoin ;
- pas d'implication du tout.

© IFACI

Reportings

L'ensemble des établissements disposent soit dans le cadre de tableaux de bord opérationnels, soit dans le cadre de leur processus Bâle 2, d'un dispositif de collectes de pertes opérationnelles incluant la fraude, d'éléments de reporting sur le risque de fraude permettant de mesurer ce risque et d'en identifier les causes et les zones de faiblesses. Par ailleurs, les équipes anti-fraude ont également entamé des travaux autour de la mise en place de reportings spécifiques. Ces travaux mettent indirectement en exergue deux constats :

- le sujet est en cours de construction pour pratiquement tous les établissements ;
- les reportings sont généralement remontés à la direction générale ou à la direction fonctionnelle (Risque, Conformité, Sécurité) de l'équipe.

En synthèse

La fraude est un sujet ancien, surtout au sein de la banque de détail et des financements spécialisées (crédit à la consommation notamment) sur lequel un regard neuf a été posé en raison des évènements récents.

Le constat principal est que tous les établissements ont décidé de dédier des équipes spécialisés à ce sujet qui demande un traitement spécifique par rapport aux autres sujets de risques opérationnels. Les lettres de mission de ces équipes sont assez semblables avec un rôle de prévention et de détection, seule la responsabilité de l'investigation diffère selon les établissements. Le rôle clé de la prévention dans le dispositif anti-fraude est également reconnu par tous les établissements, qui déploient des campagnes d'information et de formation pour leurs collaborateurs. Les techniques de détection sont assez semblables, s'appuyant principalement sur un dispositif de contrôles et de remontées d'alertes. Il faut également noter que tous les établissements ont un système de Whistleblowing, même s'il est souvent géré de manière autonome et s'il faudrait revoir son intégration avec le dispositif anti-fraude.

Au-delà de ces approches communes, les modèles d'organisation diffèrent fortement tant au niveau du rattachement hiérarchique que de l'organisation interne des équipes. Ce constat montre que la réflexion sur ce sujet est assez récente et que les modèles doivent encore gagner en maturité pour définir les bonnes pratiques. Les sujets de réflexion évoqués concernent principalement les reportings de l'équipe et l'implication des équipes anti-fraude dans les Comités nouveaux produits.

© IFACI

© IFACI

Partie IV

Le risk assesment et les procédures d'audit de la fraude

© IFACI

© IFACI

4.1 – Les modalités d'analyse des risques

Le « risk assessment » est un exercice qui est mené au moins une fois par an et dont l'objectif est la détermination du plan d'audit de l'année suivante.
L'exercice est basé sur l'évaluation des risques des différents départements de la banque (par la réalisation d'entretiens, de questionnaires ou une autre forme de recueil de données). Le risque de fraude fait partie de risques Bâle II à évaluer dans le cadre de cet exercice. Cela peut se faire via trois approches différentes : globale, ciblée ou par « scénarios ».

4.1.1 – Le risque de fraude dans le cadre d'une approche globale

Dans le cadre de cette approche, le risque de fraude est évalué au même titre que les autres risques opérationnels, en utilisant les catégories et sous-catégories Bale II.
A chaque catégorie ou facteur de risque, est affectée une note qui prend en compte la probabilité de réalisation et l'impact potentiel sur les comptes, que l'impact de réputation et réglementaire. L'ensemble des notations permet de définir une échelle d'entités risquées.
En pratique, il apparaît qu'il est souvent bien difficile d'isoler les entités les plus risquées d'un seul point de vue « fraude », les facteurs de risque opérationnel d'autre nature (commerciaux, réglementaires, etc.) se conjuguant pour déterminer la notation globale.

4.1.2 – Une approche plus ciblée du risque de fraude

Dans un environnement où le risque de fraude revêt une acuité particulière, il apparaît donc nécessaire de procéder à une évaluation distincte qui peut revêtir deux formes, d'ailleurs complémentaires, d'une part l'analyse de l'historique des pertes opérationnelles (internes et externes, survenues dans d'autres établissements), d'autre part les entretiens et les questionnaires qui seront administrés séparément de l'exercice de « risk assessment » global :

- en ce qui concerne l'historique des pertes opérationnelles ; peuvent être retenues, outre les pertes d'origine frauduleuse, celles qui sont imputables à des erreurs d'exécution, erreurs qui traduisent bien souvent des défaillances graves du système de contrôle interne ;
- pour leur part, les questionnaires sont bâtis sur la base d'une liste d'indicateurs dont des exemples vous sont proposés ci-dessous.

Les principaux indicateurs du risque de fraude peuvent être recensés selon la nature même des environnements et des attaques potentielles :

✔ *Indicateurs de fraudes internes*

Pour établir le niveau de risque de fraude lié aux différentes activités bancaires, un questionnaire peut être établi autour des notions suivantes :

© IFACI

ACTIVITÉS BANCAIRES COURANTES	
La dimension « fraude » est-elle intégrée dans la gouvernance de l'entité concernée ?	1. Les managers sont-ils attentifs au risque de fraude ? 2. Des instructions ont-elles été élaborées et diffusées aux agents concernés ? Des formations sont-elles régulièrement organisées sur le sujet ? 3. Des investigations spécifiques ont-elles été demandées/lancées récemment ? 4. Les informations relatives à la fraude sont-elles communiquées au comité d'audit ou à l'organe délibérant ?
L'organisation mise en place constitue-t-elle ou non un premier rempart contre la fraude ?	1. Les responsabilités des agents sont-elles claires, notamment en ce qui concerne la supervision des activités ? 2. La structure de comptabilisation et de reporting permet-elle un suivi détaillé des activités ? 3. Les principes de séparation des fonctions sont-ils respectés ?
Existe-t-il des facteurs spécifiques liés à l'équipe, sa composition et son évolution ?	1. Le management bénéficie-t-il d'une assez longue expérience dans le poste ou au contraire a-t-il été récemment nommé ? Maîtrise-t-il bien tous les aspects de l'activité ? 2. Le ratio de mobilité est-il élevé ? 3. L'équipe est-elle en sous-effectif ? 4. Les membres de l'équipe prennent-ils tous des congés consécutifs sur une période de 10 jours ?
La situation des comptes est-elle satisfaisante ?	1. Les comptes de la balance sont-ils régulièrement ajustés et les suspens peu nombreux ? 2. Les comptes d'erreurs et régularisations ou encore les comptes techniques et comptes de passage sont-ils périodiquement justifiés ? 3. Les comptes inactifs sont-ils régulièrement contrôlés ? 4. Les variations des résultats sont-elles expliquées par des agents indépendants des contributeurs ?
Les contrôles fonctionnent ils correctement ?	1. Les recommandations sont-elles suivies et mises en place dans les délais indiqués ? 2. L'articulation entre les différents contrôles – périodiques et permanents – fonctionne-t-elle bien ? 3. Les alertes et réclamations remontent-elles bien et sont-elles régulièrement exploitées ?

© IFACI

QUESTIONS SPÉCIFIQUES AUX BANQUES PRIVÉES	
La gestion des portefeuilles et des ordres est-elle adéquate ?	1. Les portefeuilles des clients ont-ils une rotation excessive au regard du marché ? 2. Les ordres des clients sont-ils bien documentés ? 3. Certains clients ont-ils des portefeuilles aux performances hors normes ? 4. La rentabilité du client est-elle en adéquation avec sa taille ? 5. Les ordres sont-ils affectés aux clients dans les délais prescrits ? 6. L'envoi de documentations aux clients par le front office fait-il l'objet d'une surveillance particulière ?
QUESTIONS SPÉCIFIQUES À LA SÉCURITÉ INFORMATIQUE	
Existe-t-il des mesures liées à la sécurité informatique ?	1. Les informations au sein des différents systèmes et bases de données sont-elles correctement identifiées et classées ? 2. L'état des habilitations dans les différents systèmes informatiques utilisés répond-il aux exigences de séparation des tâches et à la règle du « Need to Know » ? 3. Le renforcement des règles de séparation des fonctions/tâches permet-il de limiter la probabilité d'une action malveillante par un utilisateur non autorisé ? 4. Les flux d'information sont-ils suffisamment confidentiels afin d'éviter toute tentative d'usurpation de profil ? 5. Existe-t-il des failles au niveau de la conception des applications qui permettent de contourner les mécanismes d'autorisation et de contrôle des profils ? 6. Les gisements de données et les systèmes sont-ils paramétrés et gérés de façon à disposer d'une sécurisation suffisante ? 7. Les accès, par les informaticiens, aux données et programmes sont-ils revus, contrôlés et validés ? 8. Des mesures de sécurité informatique telles que l'utilisation d'un antivirus, d'un firewall, le cryptage des données sensibles, la protection anti-intrusion, la limitation des usages de supports externes ou de la messagerie instantanée,etc. sont-elles mises en place ? 9. Existe-t-il des procédures de détection et d'analyse des accès ou tentatives d'accès externes ?

© IFACI

✔ *Indicateurs de fraudes externes*

Des exemples de diagnostics de risque sont proposés pour trois processus : les « achats », la relation avec les gestionnaires de fonds externes et les « paiements ».

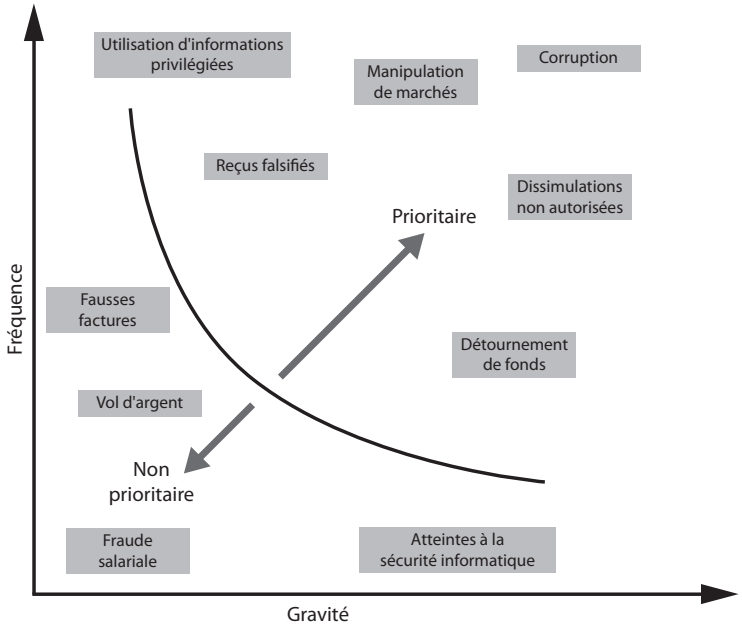
PROCESSUS « ACHATS »	
L'organisation et le contrôle des achats sont-ils satisfaisants ?	1. A quel niveau les différents directeurs peuvent-ils engager la société? 2. Existe-t-il un reporting du fractionnement des opérations ? 3. Existe-t-il une liste de fournisseurs agréés ? Sont-ils organisés par type de prestation ? 4. Existe-t-il un reporting des fournisseurs non agréés par type d'activité et par montant ? 5. A-t-on informatisé la séparation des fonctions ? 6. Les fournisseurs sont-ils fréquemment soumis à des appels d'offres ? 7. Le dépouillement des appels d'offres est-il objectif ?
PROCESSUS « RELATION AVEC LES GESTIONNAIRES DE FONDS ET HEDGE FUNDS »	
La stratégie et la performance financière des gestionnaires sont-elles suivies ?	1. Le gestionnaire est-il qualifié ? Le gestionnaire est-il expérimenté ? 2. Le gestionnaire a-t-il été capable d'expliquer clairement et de manière entièrement transparente sa stratégie ? La documentation fournie reflète-t-elle cette stratégie ? 3. Est-il possible de répliquer a posteriori la performance annoncée en appliquant la stratégie indiquée ? 4. La performance financière annoncée est-elle en ligne avec les performances du marché ? Si elle est nettement plus élevée, le différentiel de performance est-il précisément expliqué ?
PROCESSUS « PAIEMENTS »	
Le contrôle des ordres de virement est-il effectué ?	1. Y-a-t-il des ordres de virement manuel sur des comptes de clients ne faisant pas partie d'une liste pré établie et validée au préalable avec le client ? 2. Les modifications d'instructions de paiement pré paramétrées dans le système font-elles l'objet d'une autorisation expresse de la contrepartie ou du client et sont-elles validées par la hiérarchie ?

Les diverses listes d'indicateurs citées ci-dessus ne sont pas exhaustives. Elles doivent cependant rester courtes, s'agissant de diagnostics en phase d'identification des risques qui devront être approfondis par des analyses complémentaires plus détaillées.

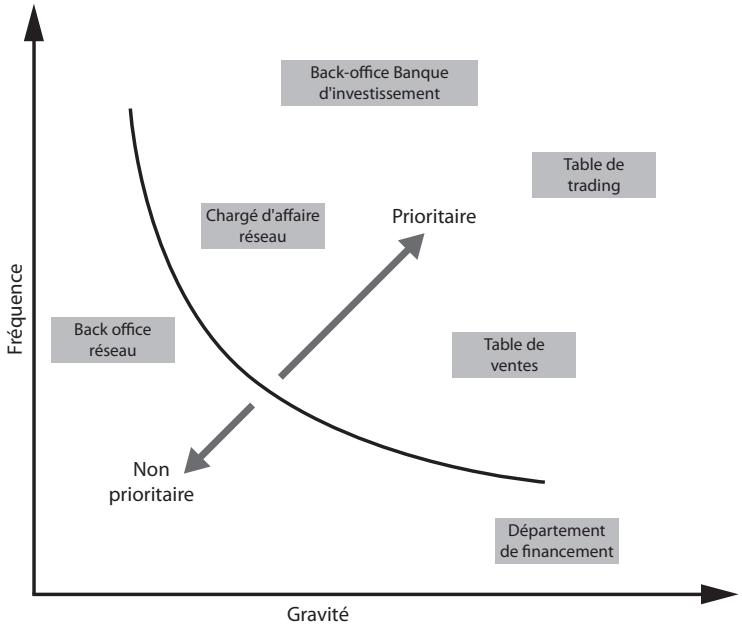
L'objectif de l'analyse à la fois des pertes opérationnelles et des indicateurs du risque de fraude est d'aboutir, en combinant ces informations quantitatives et qualitatives, d'une part à une classification des risques de fraude selon leur degré de sévérité, de l'autre à une classification des entités en fonction de leur degré d'exposition à ce risque, ce qui peut donner lieu à illustration, comme par exemple sur le diagramme ci-contre :

© IFACI

Exemple de cartographie par typologie de fraudes



Exemple de cartographie par domaines d'activité ou départements



© IFACI

4.1.3 – La méthode des « scénarios »

Cette méthode est complémentaire des précédentes. Elle permet de mieux évaluer les zones de risque et l'impact éventuel d'une fraude sur les entités ou les activités qui auront été identifiées comme présentant un risque élevé.
Les scénarios doivent être établis avec les opérationnels concernés.
Les scénarios peuvent, au-delà de la phase de « risk assessment », servir ensuite à la constitution du diagnostic ou être utilisés comme des guides de contrôle.

4.2 – Les missions d'audit et la détection de la fraude

4.2.1 – L'audit interne : une revue périodique

Pour les corps d'audit des établissements bancaires, le cadre classique d'intervention est le **contrôle périodique.** Il en découle deux implications majeures :

- en principe, le caractère espacé des contrôles (I) ;
- le fait que la recherche de la fraude ne constitue pas le fil conducteur unique des contrôles (II).

(I) *L'exercice du contrôle périodique s'inscrit habituellement dans un plan d'audit défini au préalable pour une année. Le plan d'audit doit permettre une revue régulière de chaque sous-ensemble composant l'univers d'audit, mais en raison de la taille du périmètre à couvrir, il aboutit à des* ***contrôles espacés sur chaque sous-ensemble****. Par conséquent, même s'il joue un rôle préventif indéniable dans la lutte contre la fraude (rappel à l'ordre des agents quand nécessaire, diffusion parmi les agents du sentiment que leurs activités sont surveillées, correction de failles structurelles dans les processus/contrôles par exemple), le contrôle périodique ne se substitue pas aux dispositifs permanents tels que le contrôle permanent ou, le cas échéant, les activités des équipes ad hoc dédiées à la lutte et à la prévention de la fraude (Cf. résultats de l'enquête sur les dispositifs de fraude au sein des banques, p.40). Au contraire, les deux niveaux de contrôle périodique et permanent sont tout à fait complémentaires.*

(II) *En outre, dans le cadre du contrôle périodique, les corps d'audit conduisent généralement des vérifications ayant pour objectif d'identifier aussi bien des* ***erreurs/failles opérationnelles*** *(avérées ou potentielles) que des fraudes commises par les agents. En effet, selon le règlement 97-02, le contrôle interne comprend notamment « un système de contrôle des opérations et des procédures internes ».*

Toutefois, bien que la plupart des contrôles mis en œuvre par les corps d'audit sont conçus et calibrés pour identifier en priorité des irrégularités ou des faiblesses opérationnelles sans implications frauduleuses, il incombe néanmoins à chaque auditeur **d'identifier les risques de fraude** dès lors qu'ils existent sur le périmètre audité et de **prendre en compte ce risque dans la méthode d'audit définie.**

© IFACI

A titre d'exemple, le pointage classique des factures fournisseurs (recherche de factures payées en double, de paiements effectués sans justificatif économique, pointage des RIB fournisseurs) devrait permettre d'identifier à la fois une gestion laxiste (erreurs de montant, archivage déficient, non-respect des procédures internes d'autorisation des paiements, etc.) et une fraude (circuit de fausses factures payées à une société « amie »).

4.2.2 – Les différents cadres de contrôle et leur impact sur les contrôles anti-fraude

Les types d'intervention des corps d'audit sont variés et la prise en compte du risque de fraude dépend du cadre de la mission :

- les missions classiques prévues au plan d'audit qui intègrent dans le programme de vérification, des contrôles ayant pour vocation à la fois de porter un jugement sur la qualité des processus opérationnels, le respect des procédures et de détecter des fraudes ;
- les missions transverses permettant d'évaluer la qualité de l'environnement de contrôle interne et du dispositif anti-fraude : notamment les aspects culturels et de discipline, l'audit de l'équipe anti-fraude, l'évaluation des processus de gestion des risques opérationnels (collecte des pertes, Risk Control Self Assessment-RCSA, analyse de scénario…) ;
- les missions inscrites au plan d'audit focalisées uniquement sur la recherche d'une fraude ;
- les contrôles inopinés, type « flash audit » ; un « flash audit » consiste en une revue ciblée de la mise en place et de l'application d'une ou plusieurs procédures de contrôle permanent anti-fraude dans un département donné. L'audit fournit rapidement les conclusions de cette mission, qui permettent au management de connaître la qualité de la mise en œuvre des contrôles sur ce département. Ce type de mission peut être prévu au plan d'audit ; le caractère inopiné réside dans le fait que le département ou l'entité contrôlé n'est pas précisé dans le plan d'audit et ne sait pas, par conséquent, qu'il va être audité ;
- les missions sur les règlementations anti-fraude ; dans les pays dans lesquels il existe une réglementation au niveau national (ex : anti-fraud policy au Royaume-Uni), il s'agit d'une revue de la qualité de la mise en place de cette réglementation par l'entreprise ;
- les missions d'audit informatique ; ces audits seront plus amplement développés dans le paragraphe 4.4.5. p. 66 ;
- et enfin, les missions spéciales non inscrites au plan d'audit mais lancées en cas de soupçons portant sur un agent ou un groupe d'agents, viennent compléter le dispositif (Cf. Partie V p.71).

Ces distinctions ne sont pas neutres car elles auront un impact sur les méthodes d'audit déployées, en particulier les critères d'échantillonnage : à titre d'exemple, dans un contrôle non focalisé sur la fraude, l'auditeur tendra souvent à inclure des critères de représentativité de son périmètre (en termes géographique, de produits, d'agents, etc.) alors qu'un contrôle centré sur la fraude ne prendra en compte que des critères de risque, découlant de scénarios de fraude potentielle.

© IFACI

4.3 – Les différents niveaux de contrôle

4.3.1 – La vérification de la mise en place des contrôles opérationnels

L'évaluation de la couverture des contrôles anti-fraude par des processus opérationnels permettant de réduire le risque est indispensable.

A titre d'exemple, les processus opérationnels doivent permettre la vérification de la réalité économique des opérations à travers : le contrôle des confirmations (revue du processus de confirmation des opérations aux clients et notamment s'assurer de l'exhaustivité des opérations confirmées avec les contreparties externes, mais également avec les filiales du groupe ; existence d'une procédure d'escalade des éventuelles opérations non rapprochées / des écarts constatés avec les contreparties), l'affirmation ainsi que les rapprochements internes et inter compagnies, les rapprochements front office/back office en flux et en stocks (degré d'automatisation du processus, exhaustivité des caractéristiques de rapprochement par type de produit, volumétrie des suspens, explication des éventuels écarts techniques générés par le système, analyse des suspens par nature, par montant et par antériorité, revue de l'apurement des suspens et des procédures d'escalade).

De plus, un examen des bases d'incidents doit être établi par les équipes dédiées à la gestion du risque opérationnel (Operational Risk Management).

Ces bases recensent l'ensemble des incidents, qu'il s'agisse d'erreurs opérationnelles auto-déclarées, d'événements signalés par une réclamation de clients ou de tout autre événement identifié par quelque contrôle que ce soit. Chaque item recensé doit comporter, outre l'identification des secteurs et activités concernés, un descriptif et une évaluation des montants en jeu ainsi qu'une estimation de la provision éventuelle. Un rapprochement régulier avec la comptabilité doit en assurer la pertinence.

Enfin, pour les contrôles existants, il convient de s'assurer de leur correcte formalisation par le contrôle permanent

© IFACI

4.3.2 – Les contrôles spécifiques anti-fraude

En partant des catégories de fraude présentées dans la typologie (Cf. §1.3. p.17), le groupe de travail a recensé des contrôles clés qui permettent d'identification le risque de fraude.

LES CONTRÔLES TRANSVERSAUX
1. respect de la politique interne sur la prise de congés consécutifs mais également de l'existence de backups appropriés. En effet, une fraude nécessite souvent une action répétitive du fraudeur permettant de la masquer. Or, sauf cas de complicité, seul celui-ci peut l'effectuer ; 2. vérification pour chaque agent de l'existence d'un cadre de travail spécifique à son activité et signé. Cela permet de s'assurer que chaque agent est au courant et a accepté les limites qui lui sont imposées. Ceci peut, dans une certaine mesure, rendre plus difficile le principe de rationalisation du triangle de la fraude (Cf. § 1.3.2. p.20) ; 3. respect du principe de séparation des tâches : front office / middle office / back office et fonctions de contrôle de second niveau, surtout lorsqu'il s'agit de tâches sensibles comme la gestion des paiements, la gestion des traitements manuels, les paramètres de marché, l'envoi et le matching des confirmations. En effet, l'ensemble du dispositif de contrôle interne doit reposer sur une séparation des tâches incompatibles : par exemple, un collaborateur du front office ne peut entrer des informations dans les systèmes back-office et réciproquement et celui qui ordonnance un paiement ne peut le réaliser ; 4. vérification de la cohérence de la gestion des droits d'accès et des profils alloués aux utilisateurs selon les principes de séparation des tâches : contrôler les mécanismes de délégation de droits, faire un lien entre la personne physique qui va exécuter une action pour laquelle elle a été dûment habilité et le système depuis lequel elle exécute cette action. Il convient également de s'assurer de l'existence de postes enregistrés. Maîtriser les risques d'usurpation de compte utilisateur et la confidentialité des informations d'authentification doit être assurée : chiffrement des flux d'authentification, systèmes employant des mots de passe dits « forts » (One Time Password, biométrie, etc.).

© IFACI

LES CONTRÔLES SPÉCIFIQUES

Fraudes par détournement de fonds direct ou indirect

Définition

Le détournement de fonds consiste généralement :

- soit à s'approprier directement des actifs (monétaires ou non monétaires) appartenant à la banque ou à ses clients ;

Parmi les fraudes de ce type, citons notamment le virement frauduleux, par un conseiller de clientèle, de sommes en provenance du compte d'une personne vulnérable (personne âgée, incapable majeur, personne handicapée, etc.) vers son propre compte, ou le fait de faire signer à une personne vulnérable un contrat d'assurance-vie dont le conseiller de clientèle serait le bénéficiaire (fraude conjuguée ici avec un abus de faiblesse).

- soit, à faire en sorte d'obtenir des avantages indus.

L'agent se rendra par exemple coupable de fraude dans le remboursement de ses frais professionnels : gonflement injustifié des indemnités kilométriques, présentation de dépenses à caractère non professionnel, etc).

Moyens généralement mis en œuvre

☑ la revue comptable au cours de laquelle l'auditeur se fera communiquer les justificatifs économiques des écritures comptables saisies et en appréciera le bien-fondé (utilisation des techniques de certification des comptes et de pointage d'écritures, en particulier s'agissant de la comptabilité fournisseurs) ;

☑ le pointage des virements externes émis, l'analyse globale des mouvements de trésorerie et la revue du processus de traitement des ordres émis et reçus (virements et prélèvements, transferts et rapatriements) et du processus de mise à disposition d'espèces ; une attention particulière devra être accordée aux traitements manuels :
- contrôle des habilitations du donneur d'ordre ;
- contrôle des virements téléphonés et de leur formalisation ; notamment s'assurer que l'interdiction d'utiliser des téléphones portables pour passer des ordres est respectée ;
- respect de la procédure de contre-appel systématique auprès du client pour les ordres manuels reçus supérieurs à XX K€ ; vérifier l'existence d'une piste d'audit formelle ;
- pointage des créations / modifications des coordonnées bancaires bénéficiaires dans les outils de paiement et des modifications d'instructions de paiement habituels ;

☑ le pointage des remboursements de frais professionnels ;

☑ le pointage physique des immobilisations (rapprochement entre les immobilisations enregistrées en comptabilité et les existants, afin de détecter un vol de matériel informatique par exemple).

© IFACI

Fraudes par détournement de fonds direct ou indirect *(suite)*	
	Moyens spécifiques mis en œuvre dans ...
... une banque de détail	L'auditeur interne procèdera notamment : ☑ à la saisie des valeurs (vérification inopinée de la caisse d'une agence par exemple) ; ☑ au pointage d'écritures comptables typées comme anormales (débit/crédit entre un compte client et un compte de salarié par ex.) ; ☑ à la revue des opérations des clients considérés comme « vulnérables ».
... une banque privée (ceci est valable également pour les sociétés de gestion de fonds)	En sus des risques classiques associés aux mouvements de fonds et à la gestion d'espèces, une attention particulière doit être portée à la sécurité du processus d'investissement. En effet, les gérants peuvent être incités à dissimuler les pertes enregistrées par les portefeuilles d'actifs dont ils ont la responsabilité en faussant les paramètres de valorisation ou en produisant de faux relevés de performance. Dans ce contexte, l'auditeur interne s'assurera d'abord que le gérant n'a pas la possibilité d'intervenir dans ces processus et dans le cas contraire procédera à des vérifications sur la base de la piste d'audit informatique des outils adéquats. De par le caractère proche des relations entre le chargé de clientèle et ses clients en banque privée, l'envoi de documentations (informations financières, relevées de positions, etc.) est très souvent assuré par le front office et non par un middle office. Par conséquent, il convient de contrôler que les informations fournies sont correctes et ne cherchent pas à dissimuler des pertes ou engagements non autorisés par le client. L'auditeur interne devra faire preuve d'une vigilance particulière vis-à-vis des agents de la banque qui entretiennent des relations commerciales avec des sociétés tierces : ☑ Les acheteurs constituent une population sensible (on pense ici au scénario classique dans lequel la société tierce peut chercher à influencer le choix de l'acheteur par des avantages pécuniaires ou en nature). Afin de circonscrire ce type de fraude, l'auditeur effectuera une analyse des dossiers d'achat pour en mesurer la motivation et une revue des mouvements de fonds sur les comptes des agents concernés. ☑ En outre, les agents appartenant à des sociétés de leasing et chargés de la revente des biens (voitures, camions, autobus, bateaux, etc.) sur le marché peuvent être incités à vendre ces biens à des complices à un prix inférieur à la valeur de marché, contre rémunération. L'auditeur procédera à l'analyse d'une sélection de transactions pour valider le bien-fondé du prix de cession. Il convient également de rester vigilant vis-à-vis des agents en position d'octroyer des crédits, dans la mesure où ces agents peuvent procéder à des

© IFACI

Fraudes par détournement de fonds direct ou indirect *(suite)*	
... une banque privée *(suite)*	décaissements de fonds sur la base de dossiers de crédits fictifs, octroyés à eux-mêmes ou à des complices externes contre rémunération[1]. Ce type de fraude peut être identifié en effectuant une revue traditionnelle d'une sélection de dossiers de crédit, pour confirmer notamment la réalité économique du prêt, en sus de l'appréciation du dossier au regard du risque de crédit.

Activités non autorisées ou dissimulées

Définition

Les activités non autorisées ou dissimulées comprennent :

- en l'absence d'autorisation, la prise d'engagements ou de positions sur les marchés financiers ;
- la dissimulation d'engagements compromis ou de pertes.

Exemples divers : prise de positions futures sur les marchés financiers de la part d'un trader en dehors des limites qui lui ont été accordées ; dissimulation d'un crédit accordé en l'absence de garanties ; dissimulation de pertes dues à une mauvaise gestion de positions.

Moyens spécifiques mis en œuvre au niveau

Front office / middle office	☑ le pointage des achats/ventes internes et externes de même quantité à des prix différents. En effet, ces allers-retours sur le marché, avec une contrepartie, n'ont dans la majorité des cas aucune réalité économique : cette technique de fraude permet de contrôler de manière précise le résultat généré et de dissimuler des engagements ; ☑ le contrôle des opérations hors marché ; ☑ la vérification de la réalisation et des rapprochements entre les résultats de gestion et les résultats comptables ; ☑ le pointage des transactions à départ décalé annulées ou dont certaines caractéristiques ont été modifiées (nom du client ou de la contrepartie, quantité, portefeuille, prix, dates de valeurs, etc.). En effet, un rogue-trader par exemple va chercher à détourner les limites qui lui sont imposées et compenser son résultat par un résultat fictif pour ne pas être détecté. Cela peut passer par différentes techniques, notamment via la saisie et la modification de *deals* frauduleux, qui seront annulés par le trader avant que les contrôles permettant de vérifier la réalité économique des opérations, décrits précédemment (confirmations, réconciliations, etc.) soient effectués. L'audit doit effectuer des contrôles sur les deals annulés tels que la vérification de la réalité économique des opérations annulées, et les certifications des *deals* annulés, les statistiques par trader (calcul du

[1] *Attention, notamment dans les partenariats de distribution, lorsque le crédit est monté par un agent externe à la banque (salariés d'un concessionnaire par exemple).*

© IFACI

Activités non autorisées ou dissimulées *(suite)*	
Front office / middle office *(suite)*	nombre d'opérations annulées sans justification, calcul de la position engendrée par les opérations annulées, etc.) ; ☑ la vérification de l'absence de position résiduelle dans le cas d'opérations en back to back ; ☑ la vérification du respect des limites par portefeuilles, contreparties, produits. Comme vu ci-dessus, un rogue-trader cherche à détourner ces limites par différentes techniques (saisie et modification de *deals* fictifs, qui seront ensuite annulés par le trader). L'audit interne peut comparer, d'une part, l'analyse de risque historisée à une date T et, d'autre part, l'analyse de risque de cette date T réalisée à la date du contrôle de l'audit[1]. En effet, les plus gros écarts indiqueront que des *deals* ont été annulés entre la date T et la date du contrôle de l'audit ; ☑ le pointage des paramètres de crédits et de leur modification (taux d'endettement, existence de garantie, covenants) ; ☑ le contrôle de la validité des paramètres de marché et de la fréquence de leur mise à jour ; ☑ la vérification de la validation par une unité indépendante du front office des paramètres utilisés dans la réévaluation des positions et dans le calcul des risques ; ☑ l'analyse des contrôles et résultats effectués par le service de déontologie et/ou des risques de la banque. En effet, il est important de mentionner que les contrôles cités ci-dessus ne permettent pas nécessairement et directement de soulever une fraude mais de lever des soupçons sur des agents. Il est nécessaire de croiser les informations avec notamment les résultats des enquêtes menées de façon indépendante par les équipes de déontologie afin de rassembler le plus de preuves possibles sur un ou plusieurs agents.
Back office *Voir également la vérification des contrôles opérationnels (Cf. § 4.3.1, p. 54)*	☑ la revue des comptes internes / de passage et de leur correct apurement : exhaustivité des comptes, analyse des éventuels suspens par nature et par antériorité, revue de l'apurement des suspens et des procédures d'escalade. Une attention particulière devra être accordée aux opérations en instance d'affectation par le front office à une contrepartie interne (notamment pour les sociétés de gestion) ; ☑ la revue des rapprochements des comptes nostri : fiabilité du système de rapprochement, exhaustivité, analyse des suspens par nature, par montant et par antériorité, revue de l'apurement des suspens et des procédures d'escalade ; ☑ la revue des rapprochements dépositaires : fiabilité du système de rapprochement, exhaustivité, analyse des suspens par nature, par montant

[1] *Cette technique nécessite la possibilité d'archiver les analyses de risques et de recalculer ces analyses en des dates antérieures.*

© IFACI

Activités non autorisées ou dissimulées *(suite)*	
Back office *(suite)*	et par antériorité, revue de l'apurement des suspens et des procédures d'escalade ; ☑ la revue des appels de marge en montant brut par client et par marché (cas des marchés organisés) et de manière générale, du processus de surveillance des flux de trésorerie élevés ; ☑ la vérification des frais de courtage réglés par courtier et de leur évolution dans le temps en lien avec la volumétrie des transactions traitées ; ☑ le contrôle du processus de passage en perte : habilitations et processus de validation ; ☑ la revue du processus de surveillance des comptes dormants.
Des activités de courtages	☑ identifier les pièces figurant aux dossiers des courtiers : s'assurer que les dossiers existent, qu'ils sont complets et que leur contenu est conforme aux règles définies en interne ; vérifier l'adéquation entre les données des fichiers informatiques et celles des dossiers « papiers » ; ☑ contrôler le paiement des commissions : tester la régularité des règlements effectués à certains courtiers ; s'assurer que les commissions versées concernent effectivement ce courtier et qu'elles sont calculées avec le bon taux de commissionnement ; vérifier la concordance de ces données avec les contrats ; ☑ analyser les arrêts et les changements d'activité : s'assurer de l'existence de pièces justificatives externes et internes telles que prévues dans les procédures ; s'assurer de la correcte retranscription de la démission dans le système informatique ; s'assurer de l'arrêt des paiements lorsque la prestation est terminée. ☑ analyser la nature du suivi des dossiers des courtiers : vérifier les opérations de classement à partir des numéros d'ordre des courtiers ; vérifier les pièces jointes qui doivent figurer au dossier telles que la responsabilité civile et les garanties financières qui doivent être réclamées au moins annuellement.

© IFACI

Manquements déontologiques préjudiciables à la banque

Définition

Les manquements déontologiques sont des comportements en désaccord avec les règles de conduites dictées par la déontologie. Ces règles sont émises par les autorités de régulation (Autorités des Marchés Financiers en France par exemple).

Exemples : achat d'actions en connaissance d'information privilégiées ; émission/réception de paiements vers/en provenance de pays non GAFI ; falsification de chèques.

Moyens généralement mis en œuvre

- ☑ la vérification de l'origine et de la destination des fonds lors de transferts. A noter que des opérations d'achats sur un titre, principalement sur un marché peu liquide, peut avoir pour effet un décalage successif du cours et permettre ainsi, via des transactions entre deux parties, de faire réaliser artificiellement des plus values ou des moins-values à l'une ou l'autre partie ;
- ☑ la vérification des accords KYC et pointage des transactions effectuées sans cet accord ;
- ☑ le pointage des marges excessives au regard de la politique de marge de l'établissement. Analyse des raisons légitimes en cas de dépassements de seuils ;
- ☑ le pointage des achats/ventes sur titres de mêmes quantités et mêmes prix exécutés dans la journée : l'objectif est de détecter les transactions d'achats / ventes « intraday » sans justifications économiques apparentes, les vendeurs et acheteurs agissant souvent de concert. L'objectif peut être de placer des ordres sur le marché afin de donner une impression trompeuse sur le niveau de l'offre ou de la demande au prix donné et qui sont ensuite retirés du marché avant leur exécution ou encore de donner l'impression d'une forte activité ou d'un mouvement de cours (par exemple via des wash trade) ;
- ☑ le contrôle des positions résultant d'erreurs et des résultats dégagés par les comptes erreurs ;
- ☑ le contrôle de l'affectation immédiate à un client de tout ordre stocké en compte de warehouse ;
- ☑ le pointage des transactions de tailles significatives ou dont la somme sur un même titre permet de posséder une part importante de la pose totale disponible sur le marché : l'objectif est de détecter les positions d'emprise de marché (squeeze) ou les positions très significatives et analyser les transactions nouvelles sur ces positions afin de détecter les éventuelles manipulations du prix du marché. En effet, un participant détenant une position dominante sur un produit peut l'exploiter pour modifier intentionnellement le prix auquel d'autres participants sont tenus de délivrer, recevoir ou reporter la livraison des instruments ou des produits considérés (par exemple, assécher frauduleusement le marché des prêts emprunts d'un titre donné), à l'exception de cas légitimes ;
- ☑ le pointage des transactions de tailles significatives pour compte propre passées lorsque l'agent a connaissance d'un ordre client de taille importante susceptible d'impacter significativement le prix du marché ;
- ☑ la comparaison de la liste d'initiés avec les ordres passés sur les marchés financiers : l'objectif est de détecter les transactions significatives réalisées sur la base d'informations privilégiées ;

© IFACI

Manquements déontologiques préjudiciables à la banque *(suite)*

D'après la directive sur les abus de marché, art. 2 : Une opération d'initié s'entend de « l'utilisation d'une information privilégiée en acquérant ou en cédant, ou en tentant d'acquérir ou de céder, pour son compte propre ou pour le compte d'autrui, soit directement soit indirectement, les instruments financiers auxquels se rapportent cette information ».
Le délit d'initié ne réside pas dans la détention d'une information privilégiée par une personne, mais dans l'utilisation ou la transmission de celle-ci (Cf. Annexe 2, article L. 465-1 du code monétaire et financier et article 622-1 du règlement général de l'AMF).
Dès lors qu'une personne sait ou aurait dû savoir qu'il s'agissait d'une information privilégiée, elle doit s'abstenir :
- *d'utiliser l'information pour son propre compte ou pour le compte d'autrui ;*
- *de communiquer l'information à un tiers en dehors du cadre normal du travail, de sa profession ou de ses fonctions ;*
- *de recommander à un tiers d'acquérir ou de céder les instruments financiers auxquels se rapporte cette information.*

☑ le respect de la « politique des cadeaux » pour et de la part des clients. Ceci peut se faire par exemple par la revue des notes de frais et l'analyse des montants sans justification ou au-delà d'un certain seuil ;

☑ le contrôle des chèques : Respect des diligences du CRBF 2002-01, et notamment en :
- contrôlant les chèques remis à l'encaissement, des chèques payés sécurisés ou non sécurisés (appréciation du seuil de contrôle, formalisation des contrôles de signature notamment) ;
- analysant la qualité des contrôles réalisés sur les chèques sélectionnés (contrôles des mentions obligatoires, validité du chèque, intégrité du chèque) et des anomalies détectées ;
- contrôlant la gestion des oppositions et des rejets émis (respect des délais de rejet, utilisation du code de rejet adéquat) ;
- s'assurant des déclarations au FNCI[1] de tous chèques en blanc perdus ou volés, et de la bonne tenue d'un registre.

[1] *Fichier national des chèques irréguliers.*

© IFACI

4.4 – Fraude et sécurité informatique

4.4.1 – Répartition des incidents de sécurité en entreprise

Le rapport 2008 du CLUSIF (Club de la Sécurité de l'Information Français) sur les *« Menaces informatiques et pratiques de sécurité en France »* a notamment étudié auprès d'un échantillon d'entreprises de plus de 200 salariés la typologie des sinistres liés à la sécurité informatique. Cette étude, même si elle n'est pas ciblée sur les établissements bancaires, a l'avantage de montrer l'évolution des menaces entre 2006 et 2008. Les attaques informatiques et les fraudes sont toujours les types d'incidents les moins déclarés, assez loin derrière les pannes de systèmes ou d'infrastructures, néanmoins :

- des vols ou disparitions de matériels informatiques ont été déclarés par 35% des entreprises de l'échantillon, représentant la première menace d'origine humaine directe. Même si ce chiffre est en recul par rapport à 2006, il permet de rappeler que dans le contexte de la banque, la protection contre ce type d'incidents est primordiale, les disques durs contenant fréquemment des informations confidentielles ou sensibles (données clients, données financières, orientations stratégiques) ;
- une tendance nette à l'augmentation (+50%) des attaques ciblées est observée, ainsi qu'une évolution à la hausse des incidents de divulgations d'informations confidentielles. Un type particulier de ces attaques ciblées, le *« phishing »*, en français « hameçonnage », a d'ailleurs augmenté depuis quelques années de façon significative, touchant à plusieurs reprises des établissements bancaires.

Exemple : cas réel d'attaque de « phishing » / « hameçonnage »

En début d'année 2007, environ 900 000 euros ont été dérobés à près de 250 clients de la banque suédoise Nordea, victimes d'une attaque de phishing qui a duré près de trois mois. Ceux-ci ont été incités, par mail, à télécharger et installer un filtre anti-spam, prétendument proposé par leur banque. Ils installaient en réalité un programme informatique caché (dit cheval de Troie) s'exécutant lorsque le client se connectait sur le site de la banque pour consulter son compte. La victime était invitée à saisir ses identifiants après un message d'erreur. Les informations étaient alors récupérées par les pirates, sur des serveurs situés aux Etats-Unis et en Russie.

L'impact financier a été estimé à 900 000 euros de remboursements aux clients. De plus, cet épisode a été bien sûr extrêmement préjudiciable à l'image de marque de la banque, les pertes d'opportunités en termes de nouveaux clients n'ayant pas fait l'objet d'une déclaration.

© IFACI

On peut considérer que ces chiffres sont certainement en dessous de la réalité, les entreprises étant en général moins enclines à rendre publics ce genres d'incidents, inquiètes (à juste titre) de l'impact sur leur image de marque et de la mauvaise publicité que cela pourrait générer à leur encontre.

La section suivante détaille les méthodes connues de piratage et d'attaques informatiques utilisées à des fins frauduleuses.

4.4.2 – Dommages dus au piratage informatique

Les méthodes permettant de frauder par le biais du piratage informatique ont fortement évolué ces 10 dernières années. Au-delà des tentatives d'intrusions dans les réseaux des entreprises, ce sont les techniques dites de « *phishing* » qui peuvent paraître comme étant l'une des plus grandes menaces. Ce procédé consiste le plus souvent à envoyer à des internautes un email leur demandant de se connecter à leur compte bancaire en ligne, sous un prétexte plus ou moins crédible. Le mail contient pour cela un lien vers un site internet contrefait qui imite le site original de la banque. Les pirates n'ont plus qu'à enregistrer et utiliser les identifiants ainsi récupérés et à pirater les comptes bancaires associés en effectuant des virements des transactions frauduleuses.

D'autres techniques existent. On peut citer en particulier :

- le « *social engineering* » ou ingénierie sociale. Ce terme désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courriel, courrier ou contact direct. Elle est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc. ;
- les intrusions de pirates dans les systèmes d'information afin d'y opérer des transactions frauduleuses ou de dérober des informations confidentielles qui peuvent s'échanger moyennant finance (secrets industriels ou plans stratégiques par exemple), mais aussi des coordonnées bancaires ;
- la technique dite de « *Man in the Middle* » : elle consiste pour le pirate fraudeur à se placer entre deux interlocuteurs qui échangent des informations sur le réseau et à se faire passer pour l'un et pour l'autre respectivement. L'objectif est de faire croire aux deux parties qu'elles communiquent de façon directe alors que le pirate contrôle les échanges et peut ainsi, par exemple, récupérer des données confidentielles monnayables sur le marché de la cybercriminalité ;
- le « *Spoofing IP* » ou usurpation d'adresse IP. C'est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement ;

© IFACI

- l'« *hijacking* » ou détournement de session. Cette technique consiste à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

4.4.3 – Détournement des outils informatiques à des fins frauduleuses et vol d'informations stockées sur des supports informatiques

Bien que les chiffres réels soient difficiles à établir, la plupart des spécialistes conviennent que la plus grande menace pour la sécurité provient non pas de l'extérieur, mais plutôt de l'intérieur des entreprises. De plus en plus d'employés sont tentés de frauder car comme nous l'avons vu, un véritable marché s'est développé. Il peut ainsi s'agir :

- de l'envoi par des membres du personnel de documents diffamatoires ou indécents à l'aide du système de courriel interne (pour lesquels les dirigeants de la société peuvent être tenus responsables), accompagné d'un chantage aboutissant à une extorsion de fonds. Il peut également y avoir la volonté de nuire à l'image de la société, en diffusant des informations confidentielles ou erronées, les canaux et media de publication étant plus nombreux que jamais : courriel, blogs, réseaux sociaux (Facebook, Twitter, etc.), forums Internet, etc., pour lesquels la jurisprudence est en construction ;
- d'une fraude à plus ou moins grande échelle. Détournement d'un système comptable ou financier en vue de réaliser et/ou de masquer des transactions frauduleuses : dans ce cas, le fraudeur maîtrise suffisamment le système pour profiter de failles de sécurité afin de détourner des fonds, à son profit, parfois avec la complicité de personnes internes ou externes disposant des compétences techniques nécessaires ;
- d'espionnage industriel : reventes d'informations internes et de secrets ou brevets technologiques auquel l'utilisateur fraudeur n'a pas forcément accès mais parvient à se les procurer en profitant de failles dans la gestion des accès aux dossiers partagés contenant des données sensibles par exemple ;
- de revente sur le marché de la cybercriminalité de coordonnées bancaires en masse, de numéros de cartes de crédit ou de toute information ayant de la valeur. Les canaux de fraude pouvant être l'impression sur papier d'un fichier de données sensibles ou en transférant ces données sur clé USB ou disque dur externe, voir même par email / messagerie instantanée, etc. ;
- on peut également citer le cas d'UBS, victime en 2002 d'une « bombe logique » (un code informatique malicieux mettant hors d'usage tout ou partie d'un système d'information et intentionnellement inséré dans le code source des applicatifs) : activée sur 2 000 serveurs d'UBS PaineWebber, une importante filiale du groupe financier suisse, il en aura coûté 3,1 millions de dollars pour la remise en marche du système, sans compter l'arrêt de travail

© IFACI

forcé des 8 000 brokers de la société : impact évalué alors à 50 millions d'euros mais difficilement chiffrable en termes d'atteinte à l'image et de manque à gagner.

4.4.4 – Les moyens techniques de sécurisation et de détection de la fraude informatique

L'éducation des clients et des utilisateurs est la première des mesures à prendre car trop souvent la première faille de sécurité qui va permettre une fraude est une faille humaine. La sensibilisation, le contrôle et la sanction sont tous les trois nécessaires à une prise de conscience des risques associés à la fraude informatique. Néanmoins, celle-ci existe aussi car des faiblesses et des vulnérabilités techniques et organisationnelles sont identifiées et exploitées par les fraudeurs. Cette menace grandissante pointe du doigt l'impératif d'une sécurisation des systèmes d'information des établissements bancaires :

1. l'identification et la classification rigoureuse des informations au sein des systèmes et bases de données des établissements bancaires ;
2. la gestion des droits d'accès la plus fine possible - qui a le droit ou pas de manipuler ou de lire quelle donnée ? – basée sur la classification réalisée auparavant. Le principe de base doit être le respect du *« Need To Know Basis »*, à savoir que toute information ne doit être accessible qu'aux employés ayant besoin de la connaître et/ou de la manipuler dans le cadre de leur travail ;
3. les techniques de sécurité informatique : antivirus, firewalls, cryptage des données sensibles, protection anti-intrusion, limitation de l'usage de supports externes, de la messagerie instantanée et de l'email, etc. La possibilité de faire appel à des consultants ou auditeurs externes spécialisés en sécurité informatique, pour la réalisation de tests de pénétration ou de vulnérabilité, peut être envisagée afin d'évaluer l'efficacité des mesures mises en œuvre.

Il faut bien sûr préciser qu'avant de mettre en œuvre tous ces moyens, parfois complexes et coûteux, une étape préliminaire indispensable consiste à identifier tous les actifs informatiques, les vulnérabilités associées et, in fine, les risques en découlant. Ceci afin de pouvoir cibler les priorités et d'établir un plan d'action adéquat.

4.4.5 – Le rôle de l'audit des systèmes d'informations dans la lutte contre la fraude informatique

Bien sûr, la sécurisation technique, même si elle est une condition nécessaire pour éviter la fraude, n'est pas suffisante en tant que telle. Elle doit être accompagnée d'un système de contrôle interne efficace, notamment des équipes d'auditeurs internes spécialisés en systèmes d'information qui doivent être en mesure de contrôler les processus et les méthodes de travail des équipes informatiques. Les grands principes directeurs de ces contrôles étant de :

© IFACI

- s'assurer que la sécurité fait partie intégrante d'une stratégie informatique alignée avec la stratégie métier de l'entreprise. L'audit interne, un des piliers de cette stratégie, doit être utilisé par l'entreprise comme un véritable levier pour faire progresser la sécurité informatique, par sa contribution à l'identification des failles, des risques et des moyens de les réduire ;
- revoir les méthodologies de développement en vérifiant le respect des meilleures pratiques de l'industrie informatique : séparation des tâches (recueil des besoins, spécifications, développement, tests, production), ségrégation des environnements (développement, tests, production) ;
- vérifier que des contrôles compensatoires, de supervision permanente par exemple, sont mis en place là où un risque est identifié et qu'il n'est pas possible de l'éliminer ;
- revoir périodiquement les comptes utilisateurs, les procédures associées, ainsi que la gestion des mots de passe : il s'agit d'éviter l'utilisation de comptes utilisateurs non nominatifs (donc empêchant de tracer la responsabilité), les logiciels utilisant des mots de passes trop faibles, ou bien la subsistance de comptes utilisateur d'employés ayant changé de département, de filiale ou ayant quitté la société ;
- revoir régulièrement la gestion des droits d'accès aux systèmes en production. Les évolutions des cinématiques applicatives doivent être également contrôlées afin de ne pas introduire de failles de sécurité :
  - mise en place d'interface permettant d'accéder directement aux données et de les modifier (accès aux bases de données, interfaces « *plug-ins Excel* ») ;
  - mise en place d'interface contournant les mécanismes d'autorisation et de contrôle des profils ;
  - paramétrage de sécurité des systèmes ;
  - gestion des vulnérabilités ;
- vérifier que le plan de continuité d'activité est élaboré à partir d'une analyse d'impact des métiers (Business Impact Analysis) qui prend en compte les menaces liées à la sécurité informatique.

Conclusion

L'expansion du piratage informatique ces dernières années a fait croître l'ampleur de la menace, de plus en plus motivée par les profits potentiels de la cybercriminalité. Si les moyens techniques sont la principale arme pour se protéger contre ces attaques (antivirus, firewall, systèmes de détection d'intrusion), l'éducation des collaborateurs et des clients des banques n'est pas à négliger, car souvent la naïveté humaine est la première brèche de sécurité.

Concernant l'audit et le contrôle des menaces internes, les audits techniques sont nécessaires mais pas suffisants. L'audit de l'organisation, des processus informatiques, des méthodologies et de l'environnement de contrôle doit être également réalisé périodiquement, la vision technologique n'étant pas suffisante en soi. Le lien doit constamment être fait avec les métiers supportés par les systèmes d'information, afin de prioriser les audits et contrôles sur les plus critiques pour l'entreprise.

© IFACI

De ce fait, disposer d'une équipe d'auditeurs en systèmes d'information, capables de faire le lien entre l'informatique et les activités qu'elle supporte, est un avantage majeur en termes d'efficacité du contrôle interne des établissements bancaires.

4.5 – L'utilisation d'outils informatiques dans les missions d'audit de la fraude

4.5.1 – L'extraction des données : utile et efficace sur certains types de fraudes

Dans le cadre d'une recherche ou d'une quantification de fraude, les données traitées sont issues des systèmes de stockage en place dans l'organisation. De ce fait, elles sont hétérogènes, multiples, plus ou moins structurées. En effet, l'architecture des données dans les systèmes d'information n'est a priori pas conçue dans une optique de recherche de fraude.

Ainsi une analyse « intelligente » des données est indispensable compte tenu du volume des transactions à analyser (jusqu'à plusieurs centaines de millions) et de la sophistication accrue des montages frauduleux. Un exemple en matière de prévention et de détection de la fraude sont les techniques d'analyses de données : « Data management ».

Le data management consiste à assurer et à maintenir une excellente qualité des données critiques dans les systèmes d'information de l'entreprise. En particulier les référentiels et les fichiers maîtres tels que les référentiels fournisseurs, tarifs, coordonnées bancaires, employés, paie, etc. Cette gestion des données est complétée par des extractions de données à partir de différentes applications et des requêtes « sur mesure ». Ceci permet de mettre en évidence des exceptions ou anomalies qui pourraient se révéler être des cas de fraude. A titre d'exemple, l'usage de ces techniques permet de détecter des écritures comptables ou des transactions réalisées pendant des jours fériés, un dimanche ou à des heures atypiques, en dehors des horaires usuels de travail. Elles permettent également grâce à des techniques statistiques et des analyses de distribution d'identifier des montants de transactions atypiques qui mériteraient une investigation plus poussée. Plus généralement, cette approche privilégie une analyse exhaustive de la zone de risque afin d'identifier des exceptions ou anomalies sur lesquelles porteront les investigations.

Au regard des volumes très importants de données, une telle recherche de cas de fraudes serait impossible manuellement ou par échantillonnage. Une investigation efficace nécessite des outils d'analyse de données disposant a minima de fonctionnalités de croisement de fichiers, de sélections suivant différents critères et de recherche (exacte ou floue) par mots clés.

© IFACI

Actuellement, les techniques d'analyse de données sont encore très souvent utilisées a posteriori à des fins de quantification de la fraude. Or, il est possible d'appliquer les techniques d'analyse de données à des fins de détection voire de prévention. Par exemple, en croisant les fichiers fournisseurs et les adresses et coordonnées bancaires des salariés ou en dressant des statistiques de concentration des prestataires. Les mêmes techniques peuvent être appliquées pour construire des indicateurs relatifs aux taux de remise accordés par les fournisseurs qui pourraient être liés à des achats surpayés moyennant des commissions.

Ces techniques permettent de mettre à disposition un outil évolutif capable de s'adapter au comportement du fraudeur et d'identifier un comportement ou une tendance atypique. Toute la difficulté résidera alors dans l'ajustement de la finesse des filtres mis en place pour détecter ces exceptions.

Par ailleurs, les techniques d'analyse de données contribuent à l'amélioration du dispositif de contrôle interne. En effet, les anomalies et exceptions identifiées à travers les tests d'analyse de données mettent en évidence des failles de contrôle interne telles que des contrôles non existants ou non opérants. Les analyses de données permettent ainsi de modifier ou de clarifier les politiques et procédures. Elles permettent également d'incorporer des contrôles défectifs et préventifs dans les systèmes et processus de l'entreprise.

4.5.2 – Le data mining dans la recherche de fraudes

Le data mining est un processus d'extraction de connaissances valides et exploitables à partir de grands volumes de données. Il a pour objet de transformer de « l'information » en « connaissance ».

Il a vocation à être utilisé dans un environnement professionnel et se distingue de l'analyse de données et de la statistique par les points suivants :

- contrairement à la méthode statistique, le data mining ne nécessite jamais que l'on établisse une hypothèse de départ qu'il s'agira de vérifier. C'est à partir des données elles-mêmes que sont déduites les corrélations intéressantes, le logiciel n'étant là que pour les découvrir (le data mining se situe à la croisée des statistiques, de l'intelligence artificielle, de l'analyse de données). Le data mining adopte une démarche sans a priori (approche pragmatique) et essaie ainsi de faire émerger, à partir des données brutes, des inférences que l'expérimentateur peut ne pas soupçonner et dont il aura à valider la pertinence ;
- les connaissances extraites par le data mining ont vocation à être intégrées dans le schéma organisationnel de l'entreprise ou de l'entité considérée. Le data mining impose donc d'être capable d'utiliser de manière opérationnelle les résultats des analyses effectuées, souvent dans des délais très courts. Le processus d'analyse doit améliorer la réactivité de l'organisation ;

© IFACI

- les données traitées sont issues des systèmes de stockage en place dans l'organisation et sont ainsi hétérogènes, multiples, plus ou moins structurées (logs des sites webs, données issues des terminaux mobiles, appel à un call center, retrait d'argent dans un distributeur à billets, résultats de questionnaires de satisfaction, etc). Leur raison d'être n'est donc a priori pas l'analyse de données. Cela impose de disposer de systèmes performants de préparation ou de manipulation de données.

Ainsi les techniques de data mining sont utilisées dans un objectif de détection de fraude en identifiant des comportements atypiques et anormaux. Les modèles prédictifs de comportements frauduleux sont très développés dans le secteur des télécommunications et des assurances mais également dans les organisations publiques (prestations sociales, fraudes fiscales et fraudes à la TVA).

© IFACI

Partie V

La conduite d'une mission d'investigation de fraude

© IFACI

© IFACI

5.1 – La conduite de la mission

Les investigations menées ont pour objectif de rechercher et de rassembler de façon objective tous les éléments d'appréciation nécessaires à la juste compréhension des faits.
L'enquêteur doit établir si une faute a été commise, en préciser la nature et l'importance afin d'établir l'innocence ou la culpabilité du salarié. Selon les cas, il procède personnellement aux constatations utiles, recueille les preuves matérielles puis rassemble les pièces probantes et les témoignages.
Les investigations achevées, l'enquêteur rédige son rapport. Ce dernier ne doit pas être un réquisitoire, mais un exposé objectif sur les faits, impartial sur les circonstances qui permettra de retenir des griefs adaptés aux fautes commises.

5.1.1 – Le recueil des preuves

La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation.

L'enquêteur doit établir les faits avec objectivité, pour cela il doit déterminer avec exactitude :

- la réalité de la fraude ;
- les responsabilités, celles-ci pouvant concerner à la fois la hiérarchie, les collaborateurs de la banque et des complicités extérieures ;
- les circonstances et les causes afin de déterminer les dysfonctionnements de l'organisation et d'y remédier en établissant des recommandations ;
- le préjudice financier et autre.

Pour répondre à ce quadruple objectif, l'enquêteur doit apporter les éléments de preuve nécessaires. A cette fin, il réalise des travaux spécifiques, adaptés à chaque fois en fonction du contexte tels que :

- une analyse approfondie des faits reprochés par le biais d'une étude approfondie de la comptabilité, des opérations traités (prêts, opérations de marchés par exemple) ;
- une analyse critique de la chronologie du déroulement de la fraude au regard des documents identifiés, des témoignages recueillis et des traces informatiques récupérées au sein des systèmes afin d'être en mesure de mettre en évidence des « incohérences temporelles » ;
- la recherche d'autres faits similaires et la revue des procédures sensibles dans lesquelles l'agent suspecté est amené à intervenir selon le périmètre d'activité, en fonction des habilitations informatiques ;
- une analyse des opérations bancaires de l'agent et d'autres investigations en fonction des besoins, dans le respect de la légalité.

© IFACI

Il élabore ainsi un **dossier de mission** proche de celui d'une mission d'audit classique, contenant l'ensemble des éléments de preuve de l'intégralité des faits constatés.

La bonne tenue du dossier de mission répond à plusieurs objectifs :

- tracer la piste d'audit et justifier les conclusions de l'investigation ;
- conserver les pièces originales jusqu'à transmission à l'autorité qui prendra une décision sur le résultat de l'investigation ;
- servir de base à la confrontation avec l'agent ainsi qu'au rapport de mission.

Les quatre catégories de preuve

1. ***La preuve analytique :*** *tout comme dans une mission d'audit classique, la preuve analytique est largement utilisée lors d'une mission d'investigation. Celle-ci résulte des analyses, calculs et rapprochements d'informations. Il faut toutefois s'assurer de la fiabilité et de la pertinence des données utilisées.*

2. ***La preuve documentaire*** *résulte de la collecte des documents probants sous format papier (rapports, procédures, factures, etc.) ou en format électronique (courriels, listings, requêtes informatiques, vidéosurveillance, etc.).*
   L'enquêteur est limité au seul cadre de son organisation, contrairement aux organismes d'Etat. A titre d'exemple, une mission portant sur le domaine de la lutte contre le blanchiment des capitaux ne peut comporter qu'une analyse des comptes détenus par un client au sein de l'établissement. En France, seule la cellule de lutte anti-blanchiment (TRACFIN), dans le cadre du droit de communication prévu par le Code Monétaire et Financier, ou la justice peuvent demander des renseignements aux banques ainsi qu'à certains services de l'Etat (tels que les services de police judiciaire).
   L'enquêteur peut prendre les documents originaux et les conserver définitivement ou le temps de la mission. Dès lors qu'il prend des documents, il doit en aviser la hiérarchie concernée et en laisser une copie. En fin de mission, l'enquêteur doit restituer tous les documents qui ne sont pas utiles pour la démonstration des résultats de l'investigation.

3. ***La preuve physique*** *est basée sur la constatation des faits. Ce type de preuve, très peu utilisé dans le cadre d'une investigation, n'est fiable que sous certaines conditions. Ces dernières doivent être licites, continues et entérinées par les opérationnels.*
   L'établissement peut également faire appel à un huissier de justice pour constater les faits. Cependant, les huissiers « peuvent être commis par la justice pour effectuer les constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter» . Ces constatations n'ont valeur que de «simples renseignements ».
   Si le constat d'huissier est un mode de preuve recevable, il doit cependant rester dans le cadre des attributions données par la loi. En d'autres termes, l'huissier ne peut procé-

© IFACI

der à des investigations et à des auditions de témoins, sauf si ces derniers ont pour objet de clarifier des constatations « purement matérielles ».

4. ***La preuve par témoignage : le recueil de ce type de preuves est développé ci-dessous au § 5.1.2.***

D'après L. SAWYER

Quelque soit le type de preuves, quelques règles sont à respecter :

- veiller au respect du secret professionnel ;
- respecter les règles de déontologie (réglementaires et propres à l'entreprise) ;
- s'assurer de la confidentialité des travaux : ne pas laisser sans surveillance les supports contenant les informations, ne pas consulter des informations sensibles lorsque l'environnement ne permet pas de s'assurer que ces informations ne pourront être capturées, ne conserver aucun document sur un micro-ordinateur, etc. ;
- respecter le strict besoin de savoir : ne pas utiliser ou exploiter toute information confidentielle à des fins autres que celles de l'investigation.

5.1.2 – Les entretiens

L'utilisation de l'entretien comme preuve dans une mission d'investigation n'est pas suffisant. Ce type de preuve doit toujours s'accompagner d'une validation par une preuve analytique, documentaire ou physique.

Les enjeux de l'entretien dépendent des éléments mis à jour par les investigations :

- si les preuves sont solides : l'entretien permet d'indiquer à l'agent les faits qui lui sont reprochés et d'écouter ses explications (celles-ci doivent être soutenues par des éléments tangibles fournis par l'agent) ;
- si les preuves sont plus fragiles : l'entretien est l'occasion de mettre l'agent face à ses éventuelles contradictions pour rechercher la vérité ;
- si aucun élément probant n'a pu être collecté : il vaut mieux éviter l'entretien ou se limiter à un entretien de sondage.

Dans la plupart des cas, il faut garder à l'esprit que tous les faits fautifs ou frauduleux n'ont peut-être pas été mis à jour par les travaux.

L'entretien nécessite une bonne préparation afin d'envisager tous les scenarios possible (plan de questions, réponses préparées aux arguments prévisibles de l'agent, disponibilité directe des copies de preuves). Toutes les questions devront être intégralement rédigées afin que l'enquêteur puisse se cantonner à la simple lecture de ces dernières et concentrer toute son attention sur l'atti-

© IFACI

tude comportementale de la personne interviewée. En effet, l'enquêteur peut être confronté à des interlocuteurs peu coopératifs.

Quelques règles doivent cependant être respectées :

- l'agent est convoqué par son management (absence de relation hiérarchique entre l'audit/l'inspection et l'agent) et n'est pas prévenu à l'avance de l'objet de l'entretien ;
- l'agent est rencontré seul durant ses heures de travail. Au début de l'entretien, il faut lui expliquer clairement la procédure en cours et tenter d'obtenir sa coopération ;
- l'entretien doit faire l'objet d'un compte rendu signé par l'audité : autant que possible, il faut faire valider à l'agent ses déclarations, en particulier lorsqu'il reconnaît certains faits reprochés :
  - la reconnaissance de certains faits mineurs peut l'amener petit à petit à reconnaître l'intégralité des faits ;
  - la trace écrite des déclarations rend plus évidentes les éventuelles contradictions ;
  - au fur et à mesure de l'avancement de l'enquête, la reconnaissance des faits mineurs peut ne plus présenter de réel intérêt et pourra ne pas figurer dans le rapport ;
  - en cas de préjudice pour la banque et si l'agent reconnaît les faits, l'entretien est l'occasion de lui faire signer, en même temps que les aveux, une reconnaissance de dette ;
- l'enquêteur doit toujours être assisté par l'un de ses collaborateurs ;
- au cours de l'investigation, le suspect est entendu seul sans l'assistance d'un défenseur.

L'élaboration de la grille d'entretien est laissée à l'expérience et à l'appréciation de l'enquêteur. C'est à ce dernier de provoquer, par des questions posées, soit des aveux, soit toutes explications de nature à faire la lumière sur les faits. Pour ce faire, l'ordre dans lequel seront abordés les sujets les plus sensibles est l'une des clefs de succès d'un entretien réussi. Ces derniers devront être évoqués en fin d'entretien. En effet, il convient parfois de ne pas respecter la chronologie des évènements et de revenir « incidemment » à l'occasion d'une ultime question sur le point le plus sensible de l'investigation.
Les questions ouvertes sont à privilégier. L'enquêteur ne peut orienter les réponses de l'audité : il ne peut pas prêcher le faux pour savoir le vrai.

L'enquêteur doit savoir prendre du recul face aux évènements, ne pas laisser transparaître d'émotions ou de préjugés et créer, en début d'entretien, un climat de confiance. Il doit laisser parler l'audité sans lui montrer le degré de connaissance des faits et rester neutre en toutes circonstances.

Il ne doit pas hésiter à reformuler les réponses les plus sensibles qui lui ont été apportées par son interlocuteur afin d'en valider sa correcte compréhension.

Enfin, si des contradictions apparaissent au travers des différents entretiens, l'enquêteur peut envisager de confronter les différentes personnes.

© IFACI

5.1.3 – La rédaction du rapport

A l'issue des investigations, l'enquêteur rédige un rapport. Ce dernier doit être détaillé, présenter des faits et des constats validés. En effet, le rapport sert de base à l'élaboration des sanctions et peut être diffusé aux autorités judiciaires.

Le rapport doit faire ressortir les constatations, l'analyse de l'enquêteur, les responsabilités des audités, les risques identifiés, le préjudice final, mais il peut également, si besoin, être accompagné d'une note éclairant le contexte ainsi que les recommandations quant aux mesures à prendre. Elles peuvent être d'ordre général et concerner les procédures ou l'organisation de la banque. Tous les faits doivent être consignés dans le rapport.

Il comprend les copies des pièces permettant d'apporter la preuve irréfutable des faits reprochés consignés dans le rapport.

Il doit être le plus factuel et le plus objectif possible dans la description de l'affaire pour faciliter la qualification des faits au regard des règles internes ou externes éventuellement enfreintes :

- pas de qualifications juridiques, de jugements moraux ou de valeur ;
- convaincre avec des faits, étayés par des dates, des circonstances précises, sans mêler description factuelle et interprétation des faits.

C'est un rapport contradictoire soumis à la personne mise en cause ; celle-ci se voit accorder un délai court prendre connaissance des faits et y répondre. La réponse est intégrée au rapport en annexe (pas de contre-réponse).

En aucun cas, le rapport ne doit comporter une proposition de sanction. C'est la hiérarchie du collaborateur fautif ou la direction des ressources humaines qui en ont la charge.

L'enquêteur doit faire preuve de la plus grande vigilance lors de la rédaction du rapport. En effet, ce dernier précise les noms et prénoms des collaborateurs de la banque mis en cause mais également des faits pouvant nuire à l'établissement.
Le rapport doit faire l'objet d'une diffusion restreinte. Il doit être également conservé sous deux formats : papier (de préférence dans un coffre-fort) et électronique.

5.2 – Les aspects juridiques

5.2.1 – Les opérations personnelles des agents

L'analyse des opérations personnelles (comptes et opérations effectuées) des agents par un enquêteur doit au préalable avoir fait l'objet d'une communication auprès de l'ensemble des salariés. Dans le cas contraire, l'enquêteur ne respecterait pas le droit à la vie privée du salarié.

© IFACI

Toutefois, la banque est tenue de vérifier les opérations de ses clients pour détecter les mouvements anormaux dans le cadre de la lutte contre le blanchiment des capitaux et la lutte contre le financement du terrorisme.

Enfin, la Cour de Cassation considère que « *le fait pour une banque de mettre en place un système d'exploitation intégrant un mode de traçage permettant d'identifier les consultants des comptes ne peut être assimilé ni à la collecte d'informations personnelles ni au recours à une preuve illicite* » (Chambre sociale de la Cour de cassation du 18 juillet 2000 n° 98-43.485).

5.2.2 – Les investigations sur les postes de travail

Afin de rassembler tous les éléments de preuve nécessaire à la constitution du rapport et selon le type de faits reprochés, l'enquêteur peut être amené à orienter ses investigations sur les postes de travail des salariés.

Cependant, l'enquêteur doit respecter certains principes :

- le respect des correspondances privées : l'enquêteur ne peut prendre connaissance des messages personnels des salariés de la banque. Cela constituerait une violation du secret des correspondances qui peut être sanctionné pénalement (article L.226-15 du Code Pénal). Seule une décision de justice ou une instruction pénale permettent la levée du secret des correspondances ;
- les messages non identifiés comme personnels sont présumés être professionnels ;
- les fichiers créés par le salarié sur le poste informatique mis à disposition par l'employeur sont réputés avoir un caractère professionnel, sauf s'ils sont identifiés par le salarié comme étant un fichier personnel ;
- l'enquêteur peut consulter les fichiers présents sur le poste informatique (hormis les fichiers identifiés comme personnel) du salarié sans la présence de ce dernier. Les fichiers identifiés comme personnel ne peuvent être consultés qu'en présence du salarié et avec son accord.

Il existe un moyen simple de sécuriser cette étape de travail pour éviter que le salarié ne conteste la validité de certaines preuves sous prétexte qu'elles auraient été identifiées dans sa correspondance personnelle. Il convient de réaliser une copie, devant huissier, du disque dur avant analyse ce qui permettra, à terme et si nécessaire, de localiser avec certitude l'endroit où la preuve a été identifiée.

Par ailleurs, l'employeur qui déciderait de recourir à des cabinets d'enquête externe devrait en avoir au préalable informé ses salariés. Dans le cas contraire, il pourrait y avoir atteinte au respect de la vie privée du salarié et l'employeur ne pourrait utiliser les éléments obtenus comme moyen de preuve car cela constituerait un mode de preuve illicite.

© IFACI

5.2.3 – L'utilisation des conversations téléphoniques

L'enregistrement ou l'écoute des conversations téléphoniques ne peuvent être réalisés qu'en cas de nécessité reconnue et doit être proportionnés aux objectifs poursuivis.

Pour que l'enquêteur puisse utiliser ce type de preuve, il est nécessaire qu'il s'assure auparavant qu'un certain nombre de dispositions prévues par la loi soient bien respectées :

- déclaration effectuée auprès de la CNIL, sauf désignation d'un correspondant informatique et libertés ;
- consultation des instances représentatives du personnel préalable à la mise en place du dispositif ;
- information des salariés et des interlocuteurs sur le dispositif mais également sur les conséquences qui peuvent en résulter ;
- existence d'une ligne téléphonique spécifique pour les appels privés.

Les salariés doivent être expressément informés que les conservations téléphoniques peuvent être utilisées dans le cadre d'une procédure disciplinaire.
Si ces conditions sont remplies, l'enquêteur peut se baser sur ces éléments pour étayer ses éléments de preuve.

La durée de conservation des enregistrements à des fins de preuve en matière bancaire est limitée au maximum à cinq ans, conformément aux articles 321-78 et 312-79 du Règlement Général des l'Autorité des Marchés Financiers.

5.2.4 – L'utilisation de la vidéosurveillance

La vidéosurveillance dans le milieu bancaire répond à un objectif de sécurité (contrôle des accès aux locaux, surveillance de zones de travail à risques). La mise en place d'un système de vidéosurveillance doit cependant respecter le principe de proportionnalité et doit « *s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi* » selon la CNIL.

Il est nécessaire de rappeler quelques principes de droit concernant la vidéosurveillance qui doivent être connus de l'enquêteur avant l'utilisation d'enregistrements de vidéosurveillance :

- existence d'une déclaration du dispositif de vidéosurveillance à la CNIL, lorsque le dispositif d'enregistrement vidéo fait appel à des moyens informatiques (ex : stockage des images sur support numérique, etc.), sauf désignation d'un correspondant informatique et libertés ;
- consultation des représentants du personnel avant la mise en place d'un tel dispositif ;
- information des salariés et des personnes extérieures ;
- visualisation des vidéosurveillances par des personnes habilitées.

© IFACI

A titre d'exemple, une vidéosurveillance montrant un salarié d'une banque faisant un retrait à un distributeur de billet automatique avec une carte volée n'a pu être utilisée comme preuve lors d'une mission d'investigation. En effet, il s'agit d'un dispositif installé dans un lieu public et dont l'utilisation dans le cas d'une fraude est à l'initiative de l'autorité judiciaire.

Notons enfin que la durée de conservation ne doit pas excéder le délai d'un mois.

5.2.5 – La conservation des preuves

La conservation des preuves ne fait pas l'objet d'une réglementation spécifique et dépend des normes internes définies dans l'établissement bancaire.

Les établissements peuvent se référer aux règles de prescription en matière civile (loi n°2008-561 du 17 juin 2008 portant la prescription civile à 5 ans au lieu de 30) ou commerciale (10 ans) qui exigent un impératif de sécurité juridique.

Toutefois, la durée de conservation des preuves généralement constatée est de 10 ans tels que le prévoit le Code du Commerce pour la plupart des documents (ex : factures clients, livres et registres comptables, pièces justificatives, etc.).

Dans la pratique, il apparaît le plus souvent nécessaire de récupérer et conserver un maximum d'éléments de preuve (préservation des originaux, sauvegardes informatiques avant écrasement, etc.), notamment en cas de contestation des sanctions ou de procédures judiciaires.

Le Comité Français d'Organisation et de Normalisation Bancaires (CFONB) établit un tableau sur la durée de conservation des archives. Ce tableau est en cours de refonte.

5.2.6 – Relations avec la police et les autorités judiciaires

La question du dépôt de plainte est liée à l'analyse de la nature de la fraude et de ses conséquences. Une simple erreur ou le non-respect de procédures cantonne l'affaire à un cadre réglementaire et interne. Par contre, s'il y a vol, intention de nuire, on est dans un cadre pénal. Et si l'enquête interne débouche sur des aveux, il y a lieu de porter plainte auprès des autorités, ne serait-ce que pour protéger des tiers, comme les clients.

La recevabilité des éléments de l'enquête interne, qui appuieront la recevabilité de la preuve, doit être intégrée dès le début. A ce titre, il est nécessaire de ne pas porter plainte avant de disposer d'un rapport complet et circonstancié. En effet, la plainte déposée n'entraînera pas forcément de suites ; celles-ci découleront d'une décision de l'autorité qui prendra en compte les faits exposés, leur gravité et leur qualification juridique.

© IFACI

On peut envisager de mettre en place une politique relative au dépôt de plainte, avec par exemple des seuils de déclenchement. Mais un tel dispositif sera surtout utile pour éviter de porter plainte à tout bout de champ.

Il est préférable de réserver la décision du dépôt de plainte au niveau le plus élevé de la hiérarchie afin d'assurer, à la fois, que l'ensemble des tenants et aboutissants sont pris en compte et que les conséquences sont pleinement pesées, notamment celles relatives aux tiers.
Une organisation typique consiste à prendre la décision en direction générale, sur lecture du dossier d'enquête interne et en bénéficiant des conseils de la direction juridique. A ce stade, pouvoir profiter en interne de l'expérience d'une personne connaissant les modalités d'une enquête de police peut s'avérer utile.

Une fois l'action judiciaire lancée, c'est l'ensemble des parties concernées qui est à la disposition des autorités et il faut être conscient que tout contrôle échappe naturellement à l'établissement initiateur.

Le rapport d'enquête interne et ses éventuelles annexes sont considérés comme des éléments appuyant la plainte. Ils sont utilisés pour apprécier les faits et sont versés, le cas échéant, au dossier d'instruction. Mais ils ne sauraient se substituer en aucune manière aux travaux de l'enquête de police, compétence oblige.

Les enquêteurs dépêchés par l'autorité mettront en œuvre tout moyen jugé nécessaire à leurs travaux sans qu'il y ait la moindre possibilité de s'opposer à leurs demandes. Les interrogatoires sont individuels. Hormis les collaborateurs impliqués, toute personne concernée de près ou de loin est susceptible d'être entendue ; tout salarié dont l'audition sera jugée utile pour une meilleure compréhension des faits ou de leur contexte, mais aussi des tiers, à commencer par des clients.

Il découle de ce qui précède que les insuffisances de l'établissement initiateur seront exposées, par exemple la faiblesse du dispositif de contrôle. La relation commerciale sera également impactée dans la mesure où des clients peuvent être convoqués, à l'insu même de l'établissement.

Enfin, on ne peut pas exclure que les éléments découverts au fil de l'enquête judiciaire puisse déboucher sur une autre affaire, séparée de la plainte initiale et où éventuellement l'établissement initiateur se retrouverait en position d'être incriminé. On citera à cet égard la possibilité d'une communication à des autorités de tutelle.

© IFACI

Conclusion

La lutte contre la fraude est l'affaire de tous.
Il est certainement important de le rappeler en conclusion de ce cahier consacré à la lutte contre la fraude dans le secteur bancaire et financier.

Le rôle de l'audit interne n'en est pas moins primordial, puisque sa responsabilité est bien de vérifier que les mesures préventives sont appliquées, de conduire directement des revues permettant d'identifier des fraudes, enfin, lorsque les cas sont avérés, d'en assurer l'instruction et d'établir les faits dans la perspective d'une prise de sanction éventuelle.

Au delà, le rôle de l'audit interne est bien de sensibiliser les opérationnels au risque de fraude. Dans chacun des établissements, et certainement ceux qui ont participé à l'étude, il est clair que le degré de mobilisation est aujourd'hui élevé.

Puisse ce cahier contribuer encore d'avantage à sensibiliser et former à la prévention de la fraude les opérationnels concernés !

© IFACI

ANNEXES

© IFACI

Annexe 1 : Exemples de fraudes internes dans l'octroi de crédits

Ce document résume une session de sensibilisation à la lutte contre la fraude dans une banque de détail. Après avoir identifié des dispositifs généraux de lutte contre la fraude, les participants ont analysé les risques et outils spécifiques.

Trois types de fraudes : les crédits amortissables, les découverts et avances sur un compte courant et les escomptes :

1. Exemples d'outils de prévention et de détection du risque de fraude

Politique de crédits formalisée précisant :

- la liste des produits ;
- la tarification ;
- la description du système d'autorisation ;
- les limites qualitatives et quantitatives de cette politique sont liées :
  - au profil de l'emprunteur ;
  - au chargé de dossier ;
  - au type de produit ;
- les procédures de contrôle à chaque étape de la vie du crédit, le service d'audit interne est impliqué dans ce processus.

Exploitation d'alertes telles que :

- les prêts atypiques ;
- les évolutions anormales du montant des échéances ;
- la périodicité des incidents et/ou des contentieux (remboursement anticipés, capital restant dû négatif, concours par clients excédant un certain montant, etc.).

2. Analyses sectorielles

Crédits amortissables

Les risques cités sont :

- les détournements de crédits fictifs ;
- l'octroi de crédits à des conditions préférentielles ;
- l'utilisation abusive des cautions ;
- l'irrespect des limites ;
- la divulgation d'informations sur la situation de l'emprunteur (risque relevant de l'intelligence économique).

© IFACI

Les dispositifs de lutte contre la fraude se situent aux étapes clés de gestion de crédit :

- la demande ;
- l'instruction ;
- la décision ;
- la notification ;
- la réalisation ;
- le déblocage des fonds ;
- le règlement ;
- le contentieux.

L'escompte

Les points clé pour la gestion du risque de fraude en matière d'escompte sont :

- une liste récapitulative des documents nécessaires et l'ouverture d'une ligne d'escompte (documents comptables, liste des principaux clients, renseignements complémentaires, renseignements complémentaires éventuellement de tiers, etc.) ;
- la surveillance de la qualité des signatures (rapprochement avec le fichier des incidents, cotation des signatures) ;
- la surveillance d'indicateurs afférents à la situation financière des bénéficiaires ;
- l'engagement en fonction de la surface financière du cédant (Chiffre d'affaires, rotation du cycle client et fournisseur, analyse prévisionnelle de trésorerie, etc.) ;

Découverts et avances sur comptes courants

Les dispositifs de contrôle existants permettent de limiter les incidents au niveau des découverts et des avances sur comptes courants :

- check-list des informations nécessaires à l'ouverture d'un compte courant (identité, domicile, capacité, moralité, autorisations, etc.) ;
- la confirmation de l'authenticité des copies fournies ;
- l'entrevue directe avec le propriétaire du compte ;
- l'exploitation des états d'alerte :
  - dépassement de montant d'autorisation de découvert (nombre et valeurs) ;
  - nombre de comptes débiteurs sans autorisation (nombre et valeurs) ;
  - comptes débiteurs supérieurs au plafond ;
  - modifications d'autorisation de découvert (nombre et valeurs) ;
- la confirmation des soldes débiteurs les plus importants et des dépassements.

© IFACI

Annexe 2 : Type et profil du fraudeur

Tableau 1 – Position des fraudeurs

Position	Nombre	Perte moyenne
Employé	39,7 %	70 000 $
Manager	37,1 %	150 000 $
Propriétaire / Directeur	23,3 %	834 000 $

Source : Enquête 2008 ACFE - 2008 Report to the Nation on Occupational Fraud and Abuse

Tableau 2 – Sexe des fraudeurs

Sexe	Nombre	Perte moyenne
Homme	59,1 %	250 000 $
Femme	40,9 %	110 000 $

Source : Enquête 2008 ACFE - 2008 Report to the Nation on Occupational Fraud and Abuse

Tableau 3 – L'âge des fraudeurs

Age	Nombre	Perte moyenne
Moins de 26 ans	4,6 %	25 000 $
De 26 à 30 ans	8,1 %	50 000 $
De 31 à 35 ans	12,8 %	113 000 $
De 36 à 40 ans	16,2 %	145 000 $
De 41 à 50 ans	35,5%	250 000 $
De 51 à 60 ans	18,9 %	500 000 $
Plus de 60 ans	3,9 %	435 000 $

Source : Enquête 2008 ACFE - 2008 Report to the Nation on Occupational Fraud and Abuse

Tableau 4 – L'ancienneté des fraudeurs

Année d'ancienneté	%	Perte moyenne
Moins d'un an	10,2 %	45 000 $
De 1 à 5 ans	25,7 %	100 000 $
De 5 à 10 ans	26,3 %	205 000 $
10 ans et plus	37,7 %	263 000 $

Source : Enquête 2006 ACFE

© IFACI

Annexe 3 : Cadre Réglementaire aux Etats-Unis et aux Pays-Bas

Etats-Unis

Le secteur bancaire américain est soumis à divers textes réglementaires. Les cinq principaux textes traitant de la fraude sont :

- **Crime Control Act of 1990**
- **The Securities Exchange Act of 1934**
- **The Sarbanes-Oxley Act of 2002**
- **The SEC Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) & 15(d) of the Securities Exchange Act of 1934** *(SEC 33-8810)*
- **PCAOB – AU Section 316 Consideration of Fraud in a Financial Statement Audit** *(SAS No99)*

Ces textes se complètent mutuellement afin de définir d'une part les exigences légales (civiles et pénales) et réglementaires, et d'autre part donner une interprétation et les moyens de les appliquer.

	Exigences légales	Exigences réglementaires	Interprétation	Standards (contrôle interne, …)
Crime control act (Titre XXV) *Spécifique Banque*	Renforcement des sanctions pénales en cas de fraude bancaire (fraude interne et externe)	Renforcement du pourvoir des agences fédérale en matière de régulation		
Securities Exchange Act 1934 *Spécifique Secteur financier*	Définition du cadre légale sur l'ensemble des opérations de marchés	Obligation de fournir un reporting périodique contenant l'ensemble de l'information exigible		
Sarbanes-Oxley Act *Tous secteurs d'activité*	Renforcement du dispositif légal	Contrôle interne, audit interne et externe, responsabilité de la gouvernance		Création du PCAOB

© IFACI

	Exigences légales	Exigences réglementaires	Interprétation	Standards (contrôle interne, …)
SEC 33-8810 Guidance regarding Management's report on Internal control *Spécifique secteur financier*			Guidance relatives à l'application de SOX dans le milieu financier	Référence aux dispositions de l'AICPA et COSO pour évaluer le contrôle interne
PCAOB AU-316 (SAS 99) *Tous secteurs d'activité*		Définition des normes d'audit relatives à la fraude	Identifications des risques liés à la fraude et des potentiels moyens à mettre en œuvre pour la contrer	Définition des normes d'audit relatives à la fraude mais applicables à l'audit interne

A cela s'ajoutent, nous pouvons ajouter des bonnes pratiques définies par le régulateur (OCC – The office of the Controller) notamment sur le contrôle interne et la tenue des audits internes et externes sur les différentes activités.

ANNEXE

Revue des textes

1. Crime Control Act of 1990

Le titre XXV, connu sous le nom de "the **Comprehensive Thrift and Bank Fraud Prosecution and Taxpayer Recovery Act of 1990"** élargit l'autorité du régulateur fédéral (FDIC) pour combattre la fraude. Il légifère sur le paiement de parachute doré ou toute autre forme d'indemnisation à une tierce partie affiliée. Il augmente l'amende financière et le temps de prison à l'encontre des personnes reconnues coupable de « bank crimes » et dote le régulateur de nouvelles procédures afin de récupérer les actifs soustraits à l'administration fédérale.

2. The Sarbanes-Oxley Act of 2002

- Les titres VIII et XI, aussi connus sous le nom de « The Corporate and Criminal Fraud Accountability Act of 2002 »

© IFACI

- Le titre IX connu sous le nom de « The White collar Crime Penalty Enhancement Act of 2002 »
- Le titre 3, définissant les différents engagements et devoirs du comité d'audit (et notamment au regard de la fraude Sec 301 et de la mise en place de procédures de whistleblowing)

Cet « Act » a créé une nouvelle agence quasi publique : la « Public Company Accounting Oversight Board » (PCAOB), chargée de superviser, réguler et inspecter les cabinets d'audit. Il traite également de l'indépendance des auditeurs, de la gouvernance, du contrôle interne et de l'information financière.

Les principaux titres traitant du contrôle interne / fraude sont les suivants :

- **Sarbanes-Oxley Section 302: Internal controls:**
  Il impose la mise en place de procédures internes pour s'assurer de l'exactitude de l'information financière.
- **Sarbanes-Oxley Section 404: Assessment of internal control:**
  Il impose une revue périodique du contrôle interne détaillé annuellement dans un *« internal control report »*. Les contrôles d'exactitude et d'efficacité doivent être réalisés avec l'aval du management, via des procédures internes (COSO) mais également par un audit externe (AS No 5, PCAOB). Ces deux standards requièrent, notamment de la part du management d'évaluer les contrôles destinés à prévenir ou détecter la fraude, incluant la possibilité de déjouer lesdits contrôles.
- **Sarbanes-Oxley Section 802: Criminal penalties for violation of SOX**
- **Sarbanes-Oxley Section 1107: Criminal penalties for retaliation against whistleblowers**

A noter que la SEC a publié des guidances relatives à l'application de Sarbanes-Oxley Act à l'attention du management *(Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934 du 27 Juin 2007).* Ces guidances sont comparables à celles produites par le PCAOB.

3. *The Securities Exchange Act of 1934*

Ce texte a été régulièrement mis à jour, notamment à partir de la mise en place de Sarbanes-Oxley.

⇨ **Section 10 REGULATION OF THE USE OF MANIPULATIVE AND DECEPTIVE DEVICES**

"Rule 10b-5: Employment of Manipulative and Deceptive Practices":

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality

© IFACI

of interstate commerce, or of the mails or of any facility of any national securities exchange,
(a) To employ any device, scheme, or artifice to defraud,
(b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
(c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security."

⇨ **Section 13 Periodical and other reports**

"(13e) It shall be unlawful for an issuer which has a class of equity securities registered pursuant to section 12 of this title, or which is a closed-end investment company registered under the Investment Company Act of 1940, to purchase any equity security issued by it if such purchase is in contravention of such rules and regulations as the Commission, in the public interest or for the protection of investors, may adopt (A) to define acts and practices which are fraudulent, deceptive, or manipulative, and (B) to prescribe means reasonably designed to prevent such acts and practices.
Such rules and regulations may require such issuer to provide holders of equity securities of such class with such information relating to the reasons for such purchase, the source of funds, the number of shares to be purchased, the price to be paid for such securities, the method of purchase, and such additional information, as the Commission deems necessary or appropriate in the public interest or for the protection of investors, or which the Commission deems to be material."

⇨ **Section 14 PROXIES**

(e) It shall be unlawful for any person to make any untrue statement of a material fact or omit to state any material fact necessary in order to make the statements made, in the light of the circumstances under which they are made, not misleading, or to engage in any fraudulent, deceptive, or manipulative acts or practices, in connection with any tender offer or request or invitation for tenders, or any solicitation of security holders in opposition to or in favor of any such offer, request, or invitation. The Commission shall, for the purposes of this subsection, by rules and regulations define, and prescribe means reasonably designed to prevent, such acts and practices as are fraudulent, deceptive, or manipulative.

⇨ **Section 15 REGISTRATION AND REGULATION OF BROKERS AND DEALERS**

Elle définit le régulateur comme celui qui empêche une conduite frauduleuse, manipulatrice ou trompeuse.
"The rules of the association are designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade […]"

⇨ **Section 21 INVESTIGATIONS; INJUNCTIONS AND PROSECUTION OF OFFENSES**

Elle définit le montant des condamnations financière en cas de fraude.

© IFACI

4. *SEC Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934*

(SEC 33-8810)

Il s'agit d'un guide d'interprétation à l'attention du management concernant l'évaluation du contrôle interne sur le reporting financier. Cette interprétation prône une approche dite descendante ou « top-down », orientée sur une évaluation des risques du contrôle interne qui est conforme avec les règlements 13a-15c et 15d-15(d) du Securities Exchange Act de 1934.

Le risque de fraude mentionné tout au long du document. Le contrôle interne ne peut pas détecter ou empêcher tous les cas de fraude mais ces limitations sont inhérentes au process de contrôle et il faut donc tout mettre en œuvre pour les réduire jusqu'à quasiment éliminer ce risque.

- Il est nécessaire de réaliser une évaluation du risque de fraude (revue annuellement). Elle doit être appropriée à la taille de la compagnie et à la complexité de son activité.
- Le management doit reconnaitre qu'il existe toujours un risque de fraude. Reconnaitre ce risque dans le reporting financier ne revient pas à admettre un cas de fraude, mais uniquement à prendre en considération son éventualité.
- Il est de la responsabilité du management d'identifier les risques de fraude et de mettre en place les contrôles afférents

Le texte renvoie pour les modèles de gestion du risques de fraude à :
- AICPA's 2005 Management Override of Internal Controls: The Achilles' Heel of Fraud
- COSO's July 2006 Guidance for Smaller Public Companies.

5. *PCAOB – AU Section 316 Consideration of Fraud in a Financial Statement Audit (SAS No99)*

Le document présente l'approche des auditeurs vis à vis de la fraude, ainsi que les différentes démarches à appliquer dans le cadre d'un audit. Des notions fondamentales sont précisées comme :
- l'importance de l'exercice d'un scepticisme professionnel ;
- l'évaluation de la matérialité des points d'audit liés à une fraude ;
- la sensibilisation du management ;
- la considération du risque de fraude dans les travaux analytiques ;
- la documentation.

© IFACI

En annexe de cette norme, il est fait mention de différents facteurs de risques relatifs à la fraude que sont le reporting financier frauduleux ou le détournement d'actif.

La norme propose également un extrait de guidances proposées par l'AICPA et résumées ci-dessous :

- *« Creating a culture of honesty and high ethics :*
  - *Setting the Tone at the top*
  - *Creating a positive workplace environment*
  - *Hiring and promoting appropriate employees*
  - *Training*
  - *Confirmation*
  - *Discipline*

- *Evaluating antifraud Processes and controls :*
  - *Identifying and measuring fraud risks*
  - *Mitigating fraud risks*
  - *Implementing and monitoring appropriate Internals controls*

- *Developing an appropriate Oversight process :*
  - *Audit committee / those charged with governance*
  - *Management*
  - *Internal auditors*
  - *Independent auditors*
  - *Certified Fraud Examiners »*

Bonnes pratiques de l'OCC sur le contrôle interne / Fraude

L'**OCC** (Office of the Comptroller of the Currency) intervient comme régulateur pour l'ensemble des banques sur le territoire des USA. Il a produit, entre autres, un certains nombre de bonnes pratiques sur l'activité bancaire appellées *« Comptroller Handbook »*.

- ICQs - Internal Control Questionnaires (2007)
- Internal Control (2001)
- Internal & External Audit (2003)
- Merchant Processing (2001)
- Risk management of financial derivatives (1997) …

En parallèle de l'émission de ces Handbooks, de nombreux bulletins sont émis pour préciser une évolution de la règlementation ou faire un focus spécifique sur un sujet d'actualité.

© IFACI

Working Group « Bank Fraud »

Un groupe de travail *« Bank Fraud Working Group »* a également produit en 1999 un booklet intitulé *« check Fraud : A guide to avoiding losses »* reprenant les différents cas de fraude dans le milieu bancaire et les mesures correctives à mettre en place afin d'en limiter la portée. Ce groupe était constitué de l'ensemble des agences fédérales impactées :

- FBI
- Department of Justice
- FDIC (Federal Deposit Insurance Corporation)
- FED
- IRS (Internal Revenue Service)
- OCC
- OTS (Office of Thrift Supervision)
- US Postal Inspection
- NCAU (National Credit Union Administration)
- US Secret Service

Pays-Bas

Dans un premier temps le *« Regulation on Organisation and Control »,* document émis en 1999 par De Nederlansche Bank, Banque Centrale des Pays-Bas et autorité de tutelle des établissements néerlandais, a fixé des règles applicables en matière de maîtrise des risques.

Ce texte, depuis, a été fondu dans le *« Act on Financial Supervision »* émis en 2006 sous l'égide du Ministère des Finances néerlandais et précisé par un décret royal la même année.

Il est toutefois notable que ces textes ne font pas de référence directe à la fraude en tant que telle, ni ne la qualifient. La fraude est considérée comme faisant partie du risque opérationnel avec un développement attirant l'attention sur le fait que la nature même des activités, la complexité croissante des produits, voire la pression renforcées sur les collaborateurs en termes d'objectifs accroissent les risques en général, dont ceux découlant de comportements frauduleux.

A ce titre, les autorités de tutelle néerlandaises mettent un fort accent sur la fraude interne. Cela se traduit, dans les contacts avec leurs assujettis ou lors des inspections auxquelles elles procèdent, par un soin particulier porté à la surveillance des collaborateurs et à l'adoption de processus reposant sur une stricte segmentation et une forte séparation des fonctions.

Concernant les obligations de reporting, les incidents liés aux fraudes internes ou externes doivent être signalés avec diligence aux autorités de tutelle, ainsi que les enseignements tirés et les actions correctives mises en place. Mais cette obligation entre dans un cadre général sans être spécifique à la fraude.

Quant aux sanctions, elles restent du domaine du droit pénal, même si les manquements graves en matière de dispositif de contrôle sont susceptibles d'entraîner un retrait partiel ou total d'agrément.

© IFACI

© IFACI

BIBLIOGRAPHIE

I- Dispositions réglementaires et de place

1- En France

Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement [modifié par l'arrêté du 5 mai 2009] / Commission bancaire.
Publiée au JORF n°0116 du 20 mai 2009 (page 8412)

Règlement Général des l'Autorité des Marchés Financiers. (modifié par l'arrêté du 2 avril 2009)
Publié au Journal officiel n°0081 du 5 avril 2009 (p. 6000)

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

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

Rapport au Premier ministre concernant les enseignements à tirer des événements récemment intervenus à la Société Générale / Christine Lagarde. - 2008

Directive 2008/26/CE du Parlement européen et du Conseil modifiant la directive 2003/6/CE sur les opérations d'initiés et les manipulations de marché (abus de marché), en ce qui concerne les compétences d'exécution conférées à la Commission
Publiée au Journal Officiel n°81 du 20 mars 2008 (p. 42)

Arrêté du 20 février 2007 relatif aux exigences de fonds propres applicables aux établissements de crédit et aux entreprises d'investissement Code pénal
Paru dan le JORF n°51 du 1er mars 2007 page 3796

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

Règlement du C.R.B.F. n° 2002-01 relatif aux obligations de vigilance en matière de chèques aux fins de lutte contre le blanchiment de capitaux et le financement du terrorisme du 18 avril 2002.

© IFACI

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

Code pénal
- Art. 121-7
- Art. L.226-15
- Art. 425 et suivants
- Art. 445-1 à 445-4

Code Monétaire et Financier
- Art. L. 511-41

Code du commerce

Code du travail

2- Au niveau international

Bâle II

Basel II : International convergence of capital standards : a revised Framework / Comité de Bâle. - 2005.

Principes fondamentaux pour un contrôle bancaire efficace / Comité de Bâle sur le contrôle interne. - 1998.

Framework for Internal Control System in Banking Organisations / Comité de Bâle. - 1998.

Royaume-Uni

Publications of the Financial services authority
- Financial Crime - Stakeholder Research. – 2009.
- Regulatory Notice 08-18 : Unauthorized Proprietary. – 2008.
- Prudential Sourcebook. – 2006.
- Principles-based regulation - Focusing on the outcomes that matter. – 2007.
- Guidance Notes for the financial sector / Joint Money Laundering Steering Group. – 2007.
- Financial Security Act Handbook. – 2003.

© IFACI

Legislation

Money Laundering Regulations 2007
Statutory Instrument 2007 No. 3299

Fraud act 2006.
Act of the Parliament of the United Kingdom

The Serious Organised Crime and Police Act 2005
Statutory Instrument 2005 No. 1537

The Proceeds of Crime Act 2002 (c.29) (POCA)
Act of the Parliament of the United Kingdom

Terrorism Act 2000, and the Anti-Terrorism, Crime and Security Act
Statutory Instrument 2001 No. 4019 (C. 128)

Financial Services and Markets Act 2000
Act of the Parliament of the United Kingdom

Terms and conditions of employment : Public Interest Disclosure Act 1998
Statutory Instrument 1999 No. 1547 (C. 45)

Data Protection Act 1998.
Act of the Parliament of the United Kingdom

PACE – Police and Criminal Evidence Act 1984
Statutory Instrument 2008 No. 3146

<u>Etats-Unis</u>

Sarbanes-Oxely act of 2002
Se reporter à l'« Annexe 4 : Cadre Réglementaire aux Etats-Unis et aux Pays-Bas » du présent Cahier

© IFACI

II- Référentiels professionnels et enquêtes

1- Audit interne et contrôle interne

Cadre de référence international des pratiques professionnelles de l'audit interne [CRIPP] / IIA, IFACI trad. - 2009

Fraud Prevention and Detection in an Automated World : global technology audit guide (GTAG) 13 / IIA. - 2009. (cf. p 31)

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

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

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

Position paper on the internal auditor's role in the prevention of fraud / ECIIA. - 1999

L'audit interne vers une collaboration renforcée avec ses partenaires externes / IFACI. - 1998

Audit et contrôle interne bancaire / Antoine SARDI. - 2002

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

2- Autres thèmes

Menaces informatiques et pratiques de sécurité en France / CLUSIF (Club de la Sécurité de l'Information Français). - 2008.

2008 Report to the nation : on occupation fraud & abuse / ACFE. - 2008

De la mise en œuvre des procédures de déclaration de soupçon d'abus de marché / Association des Marchés Financiers, Fédération Bancaire Française - 2008

PwC Global Economic Crime Survey 2007 : 4e enquête sur la fraude dans les entreprises en France, en Europe et dans le monde / PWC. - 2007

© IFACI

Early warning system / Hernan Murdock. - Internal Auditor du mois d'août 2003, pp. 57-61.

Arnaques : le manuel anti-fraude / Noël Pons, Valérie Berche. - 2009.

Cols blancs et mains sales / Noël Pons. - 2006

WEBOGRAPHIE

Basel Committee : www.bis.org

CEBS : www.c-ebs.org

EBC : www.ec.europa.eu

World Bank : www.worldbank.org

Beligium Banking Commission : www.cbfa.be

Financial supervision Authority of the UK : www.fsa.gov.uk

IIA : www.theiia.org

ECIIA : www.eciia.org

IFACI : www.ifaci.com

FBF : www.fbf.fr

OECD : www.oecd.org

Commission bancaire : www.banque-france.fr

ACFE 2008 report to the nation : www.acfe.com/resources/publications.asp?copy=rttn

© IFACI

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