Plans d'action et contrôles supplémentaires engagés depuis le début de l'année 2008 dans la banque de financement et d'investissement

Dès la découverte de la fraude en janvier 2008, Société Générale a immédiatement élaboré des plans d'actions afin de renforcer et d'adapter le dispositif de contrôle des activités de marché. Dans le cadre du programme baptisé 'Fighting Back', la banque a tout d'abord mis en place des mesures de rémédiation immédiates pour renforcer certains contrôles opérationnels ainsi que les conditions d'accès aux systèmes d'information. La banque a également engagé des mesures plus structurelles pour renforcer le dispositif à plus long terme. La liste intégrale des mesures est formellement présentée dans le rapport PwC publié en mai 2008. L'avancement du programme Fighting Back a été suivi régulièrement par le Comité des Comptes. Depuis, des actions de consolidation et de pérennisation des mesures mises en place se poursuivent de manière continue dans le cadre de la transformation des fonctions ressources destinée à renforcer l'efficacité opérationnelle et la sécurité de la banque de financement & d'investissement.

Synthèse des plans d'action et contrôles supplémentaires depuis début 2008

- **180M d'euros investis** sur la période 2008 - 2011
- Plus de 200 collaborateurs mobilisés sur Fighting Back et son suivi
- **Un contrôle opérationnel renforcé au quotidien selon les 4 axes** du programme **'Fighting Back'** :
    - Création du **Product Control Group** (nov 2008) responsable de la production indépendante des résultats comptables
    - Création d'un département **'SAFE'** (nov. 2008) en charge de la supervision de la sécurité des opérations financières
    - 74M d'euros investis dans le renforcement de la **Sécurité Informatique** sur plus de 180 applications sensibles de 2008 à 2011.
    - **Culture** : 8,200 collaborateurs formés au risque de fraude, mise en place de 'Principes d'action', mandats et missions des front & back offices redéfinis
- Des **engagements entièrement tenus** en termes de livrables, de planning et de budget, suivis au cours de revues trimestrielles donnant lieu à des rapports d'avancement de PwC au Comité des Comptes jusqu'en Juillet 2009

Dès la découverte de la fraude, des plans d'actions ont été immédiatement élaborés afin de renforcer et d'adapter le dispositif de contrôle des activités de marché.

Trois types de mesures ont été mis en place:

I. **Fighting Back - Mesures de remédiation** : mesures immédiates (pp 13 à 23 du rapport PwC) afin notamment de renforcer certains contrôles opérationnels ainsi que les conditions d'accès aux systèmes d'information.

II. **Fighting Back – Transformation** : mesures structurelles de renforcement du dispositif de contrôle au sens large des activités de marché sur le long terme. (pp 24 à 32 du rapport PwC)

III. **Actions de consolidation et de pérennisation des mesures mises en place.**

I. Fighting Back 1 - Mesures de remédiation

Dès la découverte de la fraude, la phase de remédiation menée par une organisation de crise a permis de circonscrire et de traiter rapidement la fraude et de mettre immédiatement en place des actions correctrices.

Cette phase s'est concentrée sur des actions prioritaires visant notamment à identifier toutes les transactions fictives liées à la fraude, à mettre en place les contrôles supplémentaires destinés à prévenir ou détecter des transactions non autorisées ou atypiques, à renforcer la supervision hiérarchique des activités du Front Office ainsi que les conditions d'accès aux systèmes d'information. Des systèmes d'escalade rapide de toute anomalie ont également été mis en œuvre.

Illustrations de contrôles supplémentaires mis en place sur:

- Les positions en nominal
- Les limites sur les '*futures'*
- Les transactions à date différée
- Les opérations internes intra Société Générale
- Les contreparties techniques
- Les modifications et annulations de transaction
- Les transactions hors marché
- La trésorerie
- Les frais de courtage

Le déploiement complet de ces contrôles s'est achevé mi 2009 sur l'ensemble des activités de trading de SG CIB et de ses implantations.

II. Fighting Back 2 - Plan de transformation

En complète cohérence avec les préconisations du rapport Lagarde, et dans le cadre d'actions plus structurelles, un ensemble de mesures a été élaboré autour de 4 grands axes :

- La création d'une entité Product Control Group et la réorganisation des Middle offices
- La création d'un département transversal, SAFE, en charge de la supervision et de la sécurité des opérations
- La sécurité informatique
- La culture et la sensibilisation au risque de fraude

1. Création de l'entité Product Control Group et réorganisation des Middle Offices

Au sein de la Direction Financière, le Product Control Group a été créé en novembre 2008 sous l'égide d'un responsable global. Il a la responsabilité de la production indépendante d'un résultat de qualité comptable, à une fréquence quotidienne et mensuelle, et de la certification du bilan.

Cette structure qui garantit une vision globale et une compréhension approfondie des activités de marché est organisée autour de 5 fonctions principales :

- production et validation du résultat économique et comptable et du bilan,
- définition/contrôle/gouvernance des principes de valorisation,
- gestion des référentiels,
- optimisation et standardisation des processus,
- contrôle interne.

Dès les premiers mois de sa mise en place, l'entité Product Control Group a eu pour priorité la mise en place d'un processus formalisé d'explication du résultat quotidien des activités de marché (Income Attribution) ainsi que la réduction des ruptures de chaîne et des écritures manuelles dans l'ensemble de ses traitements.

En parallèle, une réorganisation des middle offices a permis de clarifier les rôles et responsabilités de chacun et de renforcer l'indépendance des fonctions de support vis-à-vis des front offices.

2. Renforcement de la sécurité des opérations : création de SAFE

La Direction de la Sécurité des Opérations et de la Prévention de la Fraude, 'SAFE', créée en novembre 2008 et rattachée à SG CIB et à la Direction des risques opérationnels du Groupe, a pour but de renforcer les capacités d'analyse et de gestion des risques opérationnels de SG CIB.

Sa mission est d'évaluer de manière continue et indépendante la qualité et l'efficacité des moyens de contrôle mis en œuvre par chaque entité de SG CIB et de s'assurer de l'application des actions d'amélioration requises.

Ainsi, SAFE a notamment en charge :

- La coordination de l'ensemble du 'contrôle permanent ' (contrôle quotidien des opérations) au sein de SG CIB à travers une approche transversale couvrant à la fois les Front Offices et les Fonctions Support (informatique, opérations, finance)-et en étroite relation avec les Départements en charge de la gestion des risques et du 'contrôle périodique' (Audit et Inspection) au sein du Groupe.

- La prévention et la détection de la fraude. Outre la réalisation de contrôles inopinés par les équipes de SAFE, le dispositif mis en place repose sur deux grands principes :

    - la remontée d'"alertes" dès lors qu'un certain nombre de contrôles sensibles mettent en évidence des situations "atypiques" qui ne sont pas immédiatement justifiées ;

    - la centralisation en un point unique chez SAFE ("tour de contrôle") de l'ensemble des alertes et anomalies relevées dans le cadre des contrôles quotidiens de la banque afin d'être en mesure de détecter rapidement une éventuelle concentration sur une activité particulière et d'engager immédiatement dans cette hypothèse une investigation plus approfondie.

Par ailleurs, la sécurité des opérations a été renforcée au sein de chaque division.

3. Renforcement de la sécurité informatique

Avec 74M d'euros investis de sur 2008 à 2011, le programme de renforcement de la sécurité du système d'information de la Banque de Financement et d'Investissement a pour objectif :

- une meilleure gestion des identifiants et des droits d'accès
- une amélioration de la sécurité des applications, des postes de travail et des accès distants
- une surveillance accrue des accès utilisateurs
- le renforcement de la sécurité des données (identification des fuites d'informations) et des infrastructures.

Le projet de renforcement de la sécurité des systèmes d'information a couvert au total 180 applications sensibles, sélectionnées sur la base d'une méthodologie d'analyse de risques. Des campagnes régulières permettent la recertification de l'ensemble des utilisateurs sensibles. Par ailleurs, plus de 330 applications sont aujourd'hui connectées à un système centralisé d'authentification.

Les investissements en matière de sécurité de l'information se poursuivent aujourd'hui puisque SG CIB est la première BFI à mettre en place un système qui garantie l'identité et la traçabilité des usagés avec la mise en place de Strong Authentification. Cette solution repose sur un badge qui simplifie la gestion des mots de passe tout en réduisant les risques liés au partage de compte ou au vol de mot de passe. A ce jour plus de 11.000 collaborateurs en France et en Angleterre utilisent le dispositif Strong Authentification. Le déploiement de Strong Authentification aux Etats Unis et au sein des principales places de marché est prévu d'ici fin 2012.

4. Changement de culture et sensibilisation au risque de fraude

Ce volet inclue des actions permanentes de formation et de sensibilisation, soutenues par une communication importante à destination des managers et des collaborateurs du Groupe, et plus particulièrement :

- La diffusion et la mise en oeuvre de **principes d'action** (Business Principles), établissant un cadre de référence des comportements professionnels clairs et partagés par tous

- La mise à jour réguliére des manuels définissant **les rôles et missions** de chaque type de fonction ou métier au sein de SG CIB (lignes métiers et toutes fonctions support), ainsi que le cadre d'exercice de chacun (responsabilités, principales procédures, principes de gestion et positionnement respectifs dans la chaîne de traitement ou de contrôle). Dans le cas des traders, ce manuel est complété d'un mandat individuel encadrant son périmètre d'actions.

- De nombreuses actions de sensibilisation et de formation (notamment sur le '*rogue trading'*, les risques opérationnels) auprès de l'ensemble des collaborateurs.

Toutes ces actions sont aujourd'hui conduites sur un mode récurrent dans les missions de la Direction des Ressources Humaines et de SAFE.

Gouvernance et suivi du projet Fighting Back

La gouvernance du projet « Fighting Back » a été placée jusque fin 2009 sous l'autorité de S. Cabannes, Directeur Général Délégué du Groupe, qui présidait le comité de pilotage mensuel.

Comme exigé par le Comité Spécial du Conseil d'administration de la Société Générale, la mise en place des mesures du programme 'Fighting Back' a été assortie d'un suivi et d'un contrôle très stricts. Des revues trimestrielles effectuées de façon indépendante par le cabinet PriceWaterhouseCoopers ont permis de vérifier l'état d'avancement de l'ensemble des actions. Les rapports et conclusions ont été remis et discutés systématiquement au Comité des comptes de la banque, avec information du Conseil d'Administration.

Les résultats de Fighting Back

L'Inspection Générale a réalisé début 2009 une mission d'audit du plan d'actions « Fighting Back » qui a confirmé sa pertinence et son exhaustivité au regard des faiblesses identifiées dans le cadre de l'enquête sur la fraude exceptionnelle, et une autre fin 2009, visant cette fois à s'assurer de la complète mise en œuvre des actions, dont les conclusions ont été publiées début 2010.

L'ensemble des engagements pris en mai 2008 par la banque ont été tenus.

III. Pérennisation et amélioration continue du dispositif de contrôle

Les contrôles et mesures mis en place dans le cadre du programme 'Fighting Back' font maintenant partie intégrante du dispositif global de contrôle des opérations de SG CIB et continuent à faire l'objet d'améliorations régulières. Une nouvelle étape est aujourd'hui en cours : la pérénisation et l'amélioration continue du dispositif de contrôle.

Afin d'optimiser le dispositif et l'adapter à l'évolution de l'organisation de SG CIB, le programme CO.S.I. (Convergence, Sécurisation et Industrialisation) a été lancé au second semestre 2009. Il a notamment pour objectif :

- la convergence et l'optimisation des procédures de contrôle « Fighting Back »,
- l'industrialisation, la sécurisation et la convergence des systèmes d'information supportant le dispositif,
- l'intégration de nouveaux contrôles dans le dispositif « Fighting Back » afin d'étendre le périmètre des scénarios de fraudes couvert pas ce dispositif,
- l'industrialisation de l'outil permettant la centralisation des situations "atypiques" (Tour de contrôles).

SG CIB procède désormais à la transformation en profondeur de son modèle opérationnel en optimisant et industrialisant ses processus, et continue à investir afin de renforcer encore son contrôle des risques et la sécurité de ses opérations.

L'ensemble des actions correspondantes contribuent à renforcer encore la maîtrise du risque de fraude, via la simplification et la standardisation du dispositif opérationnel, et sont suivies dans le cadre du programme stratégique Ambition SG 2015 du Groupe.

.