Institut de l'Audit Interne

LES RENCONTRES DU GROUPE PROFESSIONNEL « BANQUE »

LES MISSIONS D'AUDIT :
LES FIGURES IMPOSEES DANS LE SECTEUR BANCAIRE

MARDI 19 JUIN 2007

Louis VAURS

Le groupe Banque est, comme vous le savez, présidé par Patrice Josnin, adjoint de l'inspecteur général de BNP Paribas. Il est, en outre, président du *Banking Advisory Group*, le seul groupe existant dans le cadre de la Confédération Européenne des Instituts d'Audit Interne (ECIIA). Je lui donne la parole.

Patrice JOSNIN

Le but de cette réunion est d'échanger, de partager nos préoccupations, de faire part de nos expériences, des difficultés auxquelles nous nous heurtons, des questions que nous nous posons. Il est très important qu'il y ait un enrichissement mutuel.

Trois intervenants animeront le débat :

- Claire Valtot-Cochard, responsable de l'audit d'ABN-AMRO France ;
- Frédéric Geoffroy, responsable de l'audit de la SGIB (*Société générale Investment Banking*) ;
- Michel Le Masson, inspecteur général de CALYON.

Ils aborderont **cinq thèmes :**

1. **Bâle II ;**
2. **Risque de conformité ;**
3. **MIFID ;**
4. **Activités externalisées ;**
5. **PCA.**

Je voudrais, très rapidement, faire quelques remarques sur le thème central de cette réunion : les missions d'audit interne : les figures imposées du secteur bancaire.

Ce titre sous-entend qu'en matière d'audit interne il y aurait des figures libres et des figures obligatoires. Si, en partant de cette constatation primaire, on va un peu plus loin, on peut en déduire qu'il existe deux approches opposées dans nos plans d'audit, dans nos démarches : la démarche qui procède de l'approche par les risques (c'est la démarche de base de l'auditeur), et une démarche beaucoup plus administrative consistant à conduire des audits pour répondre à une disposition réglementaire du régulateur. Et il est vrai, on le sait bien dans nos établissements bancaires, que le régulateur nous impose de plus en plus de travaux, d'exercices réglementaires, auxquels nous consacrons une part importante de notre temps et de nos moyens. J'ajoute qu'il y a une convergence internationale de cette tendance.

En poussant encore plus loin le raisonnement, on pourrait se demander si l'audit bancaire n'est pas soumis à une nouvelle règle de gouvernance. Nous avons été longtemps rattachés exclusivement à l'organe exécutif, dans nos entreprises, et progressivement, un tropisme (sans nous détacher bien entendu de la tutelle hiérarchique de l'exécutif), nous a rapprochés de l'organe délibérant, soit directement du conseil d'administration, soit du comité d'audit qui est une émanation du conseil d'administration. Est-ce que le mouvement ne se poursuit pas en pointillés et de façon très douce, mais néanmoins perceptible, avec le régulateur, parce que le régulateur fait partie de ceux qui régissent quelque peu l'organisation de l'audit ?

Je tiens volontairement des propos un peu caricaturaux pour faire ressortir le maître fil qui va sous-tendre l'ensemble des présentations.

Le thème d'aujourd'hui peut se décliner en trois questions gigognes.

- Figures libres et figures imposées de l'audit interne : y a-t-il une différence de nature ?
- Les exigences du régulateur en matière de mission d'audit, renforcent-elles ou contredisent-elles notre approche traditionnelle et obligée par les risques ?
- L'audit interne bancaire est-il devenu un auxiliaire du régulateur ?

Pour répondre à ces questions, nous allons voir comment ces exercices obligés s'insèrent dans nos plans d'audit et quelles en sont les éventuelles conséquences organisationnelles sur nos équipes.

Nous allons commencer par la thématique de Bâle II qui est au cœur de notre actualité et totalement incontournable.

Je rappelle l'historique de Bâle II. En 1988, le Comité de Bâle a instauré un nouveau cadre que l'on appelle l'accord de Bâle, qui arrête les exigences minimales de fonds propres. C'est le fameux ratio Cooke (8 % des engagements pondérés). Ce ratio s'applique d'abord aux membres signataires de l'accord, puis, très vite, il va s'appliquer aux banques d'une centaine de pays. Il sera modifié en 1996 pour intégrer le risque de marché, puisqu'au début il ne concerne que le risque de crédit.
On se rendra compte au bout de quelques années que cet accord de Bâle – dit Bâle I – est incomplet, et insuffisamment différencié : il aborde trop globalement les risques de crédit ; des risques, comme le risque opérationnel, ne sont pas pris en compte.
Le Comité de Bâle se réunit à nouveau à partir de 1999, et un nouvel accord de Bâle institue le ratio McDonough. Cet accord sera publié en 2004 avec une nouvelle version en 2006.

C'est un domaine où l'audit a un rôle important à jouer, et Michel Le Masson va nous rappeler les attentes du régulateur à notre égard.

Michel LE MASSON

Le cas de Bâle II par rapport au thème général décrit par Patrice est intéressant, parce que même si, dans le futur, cela deviendra un élément récurrent de notre plan d'audit, au départ ce n'est pas le cas. En effet, dans le cadre de la mise en place du programme Bâle II et avant de valider le processus d'homologation, le régulateur a demandé à l'ensemble du secteur bancaire d'intervenir dans le mécanisme de pré validation du dispositif Bâle II.
Au fond, que demande le régulateur ? Il demande aux inspections de vérifier que le dispositif réglementaire, défini dans les textes de Bâle mais sur lequel il n'y a pas encore de jurisprudence bien établie, est mis en place dans le secteur bancaire.
Quand nous avons dû organiser le dispositif d'audit pour couvrir ce domaine, nous ne disposions que des guides, assez généraux, établis par le régulateur, et qui étaient une façon de lire la réglementation Bâle II. Nous ne disposions pas d'un guide d'audit précis sur le sujet.
De ce point de vue, Bâle II est donc un élément qui sort du cadre habituel, c'est-à-dire du cadre de notre plan d'audit traditionnel basé sur les risques, même s'il y a un lien évident sur lequel je reviendrai. Le régulateur sous-traite aux inspections générales un exercice de prévalidation pour lui permettre d'intervenir en s'assurant qu'un certain nombre de points auront été vérifiés par les inspections internes. Il faut voir là un signe de confiance du régulateur à l'égard des inspections bancaires.

La mise en place du dispositif de Bâle II, a nécessité une mobilisation très importante de ressources dans l'ensemble des inspections.
Pour l'inspection dont j'ai la charge, sur l'exercice 2006 qui était l'année sur laquelle nous avons fait le pré-examen de la Commission bancaire, j'ai mis environ 50 inspecteurs sur le dispositif pendant 12 semaines, c'est-à-dire à peu près l'équivalent de 3 000 jours/homme et à peu près 1/3 de nos ressources d'audit, l'essentiel de ces ressources étant concentré sur l'exercice crédits, puisque l'aspect risques opérationnels est un peu moins lourd à traiter.

Il est évident que quand, sur une année, on doit affecter une part aussi considérable de son dispositif de ressources sur une mécanique de prévalidation pour le régulateur, on peut se demander si en faisant cela on n'est pas en train de soustraire des ressources qui feront défaut pour le reste de la couverture traditionnelle de notre risque d'audit. Est-on bien dans notre rôle en faisant ce travail de prévalidation pour le régulateur ?

La mise en place de Bâle II, nous a amené à revoir la méthodologie et les processus, ce qui a été souvent bénéfique. Nous avons vérifié tous les aspects de gouvernance en matière de suivi du projet, nous avons pris conscience de l'importance de la transversalité de ce projet en interne et de son caractère éminemment structurant, puisqu'il conduisait à passer au scanner toute l'organisation de la banque, des bases tiers au système de risques en passant par tous les mécanismes de production d'analyse de crédits, de décision…L'investissement s'est révélé rentable. Sans Bâle II, de nombreux chantiers n'auraient pas été menés à bien et aussi vite ; beaucoup de recommandations faites au cours de nos missions d'audit n'auraient pas été prises en compte.
Bâle II a aussi conduit l'audit à mener des missions beaucoup plus complexes avec une meilleure organisation du travail.

Maintenant que nous sommes au bout de ce processus d'homologation, puisqu'il s'achèvera à la fin de l'année 2007, comment va-t-on se projeter dans le futur en tenant compte de cette dimension Bâle II dans nos plans d'audit ? Désormais deux thèmes doivent être pris en compte. Le premier concerne l'évaluation des modèles de risques. Sur ce point la Commission bancaire est assez claire, s'étant penchée sur ces modèles dans la phase de validation. Elle attend que les équipes d'inspection interne des banques, sans le support de concours externes comme cela a pu être le cas pendant la phase de prévalidation, s'approprient cet audit des modèles, ce qui veut dire un exercice, des profils différents de ceux que l'on avait l'habitude de trouver parfois dans les équipes d'audit. C'est une dimension nouvelle du plan d'audit qu'il faudra intégrer : la capacité des équipes à évaluer les modèles de risques, de façon très mathématique, très professionnelle, qui sort des figures que l'on avait l'habitude de faire de façon traditionnelle.
Le deuxième thème concerne tout ce qui va être l'audit de ce que l'on appelle l'usage, c'est-à-dire le bon déploiement du dispositif et sa réelle utilisation. Cela va faire partie des figures imposées.

Je dirai pour conclure sur Bâle II que oui, certes, c'était une figure imposée ; mais c'était une figure imposée indispensable parce que, au travers de Bâle II, c'est l'ensemble du dispositif des risques de la banque que nous sommes amenés à auditer de façon beaucoup plus structurée, plus professionnelle, avec des outils que l'on n'avait pas forcément l'habitude d'utiliser dans le passé.

Patrice JOSNIN

Merci, Michel. Est-ce que tout le monde partage cette vision finalement très positive ?

Michel LE MASSON

Elle est très positive après coup, parce que l'on a plus de recul.

Question dans la salle

Je voudrais savoir, pour l'audit des modèles, ce qui est prévu dans vos plans ? Est-ce que ce seront des revues annuelles ou sur des cycles plus longs ?

Michel LE MASSON

Le régulateur s'attend à des revues annuelles. D'ailleurs, ce n'est pas propre à la France. Il faut que ce soit fait maintenant sur une base régulière.

Louis VAURS

Je voudrais poser une question à Claire Valtot, parce que je suis étonné du nombre d'auditeurs qui ont été mobilisés pour cette opération. Je crois savoir que la Société générale, comme la BNP, n'étaient pas des organismes soumis à SOX. En revanche, je pense qu'ABN-AMRO l'était. Donc, je voudrais savoir comment l'audit interne s'est réparti le travail entre Bâle II et la mise en place de SOX.

Claire VALTOT

En fait, il y a deux questions en une. La première question est : dans le cadre du dispositif Bâle II, quel effort de guerre le groupe audit de l'ABN-AMRO a-t-il dû fournir ? La réponse est : environ 15 auditeurs à temps plein, avec des pointes à 25 en central, c'est-à-dire au siège social à Amsterdam, plus la contribution des unités délocalisées, comme la mienne par exemple, pour la validation des bases de données, entre autres.
Evidemment, comme le disait Michel, cela demande des compétences. La plupart de ces compétences ont été trouvées à l'extérieur. Avec mes collègues d'Amsterdam, nous avons fourni d'énormes efforts de recrutement et de formation interne pour monter et mettre à niveau une équipe qui tienne compte des exigences internationales.

La deuxième question a trait à SOX. Pour ce qui me concerne, SOX, à Paris, représente 1,5 auditeur à temps plein, sur une équipe de 15 auditeurs.

Ce sont deux efforts parallèles, SOX portant essentiellement sur la validation des données financières et les dispositifs de contrôle permettant de produire l'information financière, et Bâle II portant sur les dispositifs de détermination des risques.

Patrice JOSNIN

Je voudrais vous poser, à vous tous, une question concernant l'audit des modèles. Je voudrais savoir si, dans vos établissements, d'une manière générale, les modèles sont audités par vous-mêmes ? Est-ce externalisé ? Si c'est fait par vous-mêmes, qu'est-ce que vous auditez ? Les données introduites dans le moteur ou l'algorithme du moteur ? Est-ce que quelqu'un peut témoigner sur ce sujet ?

Un participant dans la salle

En termes de modèles, les choses sont très diverses entre des modèles à dire d'expert, sur des métiers du genre shipping, aéronautique – pour lesquels à mon avis il est difficile de trouver des auditeurs vraiment expérimentés – et tous les modèles plus statistiques, sur lesquels il est plus facile, pour les inspections générales d'une certaine taille, d'avoir en permanence chez elles un certain nombre d'ingénieurs tout à fait capables d'auditer une série statistique.

Michel LE MASSON

On ne sait pas encore comment résoudre cette question, parce qu'il s'agit de compétences dont on ne dispose pas en interne dans les équipes d'audit. D'ailleurs, la Commission bancaire l'a reconnu en disant que ceux qui sont capables de faire ces audits des modèles dans les établissements, sont ceux qui étaient en train de les faire. En général, ils n'étaient pas chez nous, ils étaient plutôt du côté des structures de risque.
C'est un premier élément de réponse, un élément nouveau à intégrer : nous n'avons pas les compétences, en interne, pour faire cela. D'autant qu'il faut aussi avoir une taille critique suffisante pour pouvoir amortir des équipes de cette nature, avec des profils spécialisés ; un petit établissement ne peut pas avoir un auditeur spécialisé dans les modèles.
Les compétences en interne, aujourd'hui, existent chez ceux qui étaient en charge de mettre en place Bâle II, pas d'auditer les modèles. Il y aura peut-être une deuxième étape où ceux-là voudront changer de métier et se mettre du côté de l'audit.
Mais dans la première phase, je pense que beaucoup d'établissements ont recours à des cabinets extérieurs pour les aider à valider cette étape.
Cela dit, la Commission bancaire a été très claire : elle attend des grands établissements qu'ils mettent les moyens pour internaliser cette fonction, parce que cela fait partie du cœur du moteur ; ce ne sont pas seulement les données et leur intégrité, c'est aussi le moteur lui-même et son fonctionnement.

Patrice JOSNIN

Je confirme ce que tu viens de dire. Chez BNP Paribas, une équipe a été constituée à l'inspection générale – pour l'instant, elle est encore assez légère – sous la responsabilité d'un normalien mathématicien. Cette équipe indépendante est chargée de regarder le cœur du moteur, ce qui n'empêche pas que la direction des risques elle-même, comme tu l'as bien dit, a son équipe totalement indépendante des autres équipes de risque, pour développer et tester le modèle.

Frédéric GEOFFROY

L'organisation est la même pour la Société générale. Les équipes d'inspection ont travaillé avec les équipes de risques. Il n'y a pas de différence avec ce qui vient d'être dit par BNP et Calyon.

Patricia LANTZ

Ce que vous avez dit est très important mais je crois qu'on a oublié un intervenant qui est le contrôle permanent. La Commission bancaire y attache énormément d'importance et l'on doit travailler beaucoup, à notre niveau, avec les équipes de contrôle permanent des directions des risques, distinctes de celles qui fabriquent les modèles et qui sont là pour les valider, comme le prévoit la réglementation. Et c'est vrai que plus ces équipes-là sont fortes et indépendantes en interne dans les directions des risques, plus notre travail d'auditeur est facilité.

Je pense que jusqu'à présent, dans certains établissements, la Commission bancaire a trouvé que certaines équipes de contrôle permanent ou de contrôle des équipes de validation, avant l'intervention des inspections générales, étaient peut-être un peu faibles, et elle a pu faire peser sur les inspections générales un certain nombre de demandes, parce qu'elle ne trouvait pas d'équipe de validation très pointue.

Je crois que l'exemple de la BNP qui a une cellule de certification des modèles à la direction des risques, mais indépendante de celle qui les fabrique, est un modèle très intéressant pour l'ensemble des groupes bancaires.

Patrice JOSNIN

Merci d'être intervenue, et d'avoir souligné que le contrôle permanent et sa robustesse sont essentiels dans cette démarche.

Nous allons maintenant aborder le deuxième thème qui constitue aussi un exercice obligé. C'est le thème de la conformité.
La conformité est un sujet vaste et complexe. La première complexité vient de la difficulté à en définir le périmètre.

Une enquête a été conduite auprès d'un large panel d'établissements bancaires, l'année dernière, par Ernst & Young ; elle a été publiée en septembre 2006.
Ernst & Young distinguent trois catégories, trois cercles concentriques constitutifs du périmètre de la conformité.

Le premier cercle, le plus petit, ce sont les sujets incontournables. Ce sont les lois sur les crédits et l'épargne, la réglementation AMF, la lutte contre le blanchiment, les abus de marché et le conflit d'intérêts.
Le deuxième cercle, un peu plus large, est appelé par Ernst & Young les sujets partagés, parce qu'ils sont partagés avec d'autres fonctions (juridique, fiscale, etc.). Cela concerne notamment les obligations prudentielles, la surveillance des risques, la CNIL, etc.
Le troisième cercle ce sont les sujets ouverts (fiscalité des produits, droit des contrats…). Selon les établissements, ces sujets figurent tantôt dans le périmètre de la conformité, tantôt ils n'y figurent pas.

Si le sujet est considéré comme majeur par tous les établissements – et il ressortait d'ailleurs de l'enquête qu'il est considéré comme un sujet de direction générale –, ceux-ci n'ont pas adopté la même définition et ne donnent pas la même couverture. De ce fait, les dispositifs mis en place présentent des disparités assez importantes.

Michel LE MASSON

Le risque de non-conformité est un risque à la fois ancien et récent, difficile à appréhender mais incontournable. Tous les établissements, tôt ou tard, seront confrontés à cette problématique de la conformité, parce que le métier devient très compliqué. Dans des organisations multiproduits, multipays, qui doivent satisfaire à des réglementations de plus en plus complexes, c'est un risque auquel on ne peut pas échapper.
On ne le considérait pas de la même façon il y a dix ans, c'était un risque peu connu ou peu appréhendé en tant que tel. Le nouveau règlement 97-02 a fait de ce risque de non-conformité un élément fondamental du dispositif prudentiel. Et nous, en tant qu'auditeurs internes, devons veiller à ce qu'il soit couvert.

Comme l'a dit Patrice en introduction, ce risque recouvre beaucoup de thèmes. D'autre part quand on parle du régulateur, il y a plusieurs régulateurs : la Commission bancaire et l'Autorité des Marchés Financiers en France ; et à l'étranger, ce sont les multiples réglementations dans les différents pays où l'on exerce.
C'est donc un risque extrêmement vaste, très touffu, très complexe, avec une réglementation de plus en plus détaillée qu'il est difficile d'appréhender de façon synthétique et globale en même temps, dans les établissements exerçant des activités variées dans différents pays.

Parmi les thèmes énoncés, certains sont anciens comme le blanchiment. Il y a eu un durcissement très net de la part de tous les régulateurs, dans un contexte international tendu. La problématique du blanchiment concerne tous les établissements, quelle que soit leur activité : banque de détail, d'investissement…
Et puis il y a des thèmes nouveaux, comme les abus de marché, pour lesquels le régulateur attend que les établissements déploient des outils sans que ce soit expressément explicité

dans la réglementation. D'où la difficulté pour nous auditeurs, de trouver le bon réglage de ce que nous devons intégrer dans notre plan d'audit.

Cela dit, retenons que le régulateur en a fait un élément essentiel de son dispositif de surveillance. En tant qu'auditeurs, nous sommes là pour prévenir les risques de notre établissement. Le risque de non-conformité est certainement un des plus importants auxquels les établissements sont aujourd'hui confrontés. Donc, du point de vue de l'audit, il faut l'intégrer de façon beaucoup plus systématique et récurrente dans notre plan d'audit que cela n'était fait dans le passé.

Comment couvrir le risque de non-conformité ? D'abord, par des missions thématiques (contrôle de *know your customers*, par exemple)
Ensuite, dans la quasi-totalité des types de missions, on fait des recommandations touchant à la conformité qui sont souvent des recommandations du niveau le plus élevé, et devant attirer l'attention de la direction générale.
Enfin, il convient d'auditer les structures qui sont en charge de la conformité, ce qui n'est pas toujours facile. Mais ces structures récentes font partie du dispositif de contrôle et doivent donc être auditées comme toutes les autres fonctions.

Le risque de non-conformité devant être maîtrisé en permanence, il faut faire le lien avec le contrôle permanent. Auditer le risque de non-conformité périodiquement, par le biais d'audits programmés, n'est pas suffisant. Il faut donc – et c'est toute la logique du nouveau règlement 97-02 – conforter l'audit en termes de contrôle de dernier niveau. Si le contrôle permanent fait bien son travail, si la conformité fait bien son travail, c'est-à-dire qu'ils intègrent la dimension contrôle dans leur dispositif au quotidien, ils feront des tests, un certain nombre de vérifications que l'audit avait l'habitude de faire dans le passé, et qui permettront à l'audit de se pencher sur le fonctionnement et la gouvernance du dispositif. Bien sûr, l'audit devra faire aussi des tests pour s'assurer que le risque de non-conformité est bien couvert. On s'aperçoit, en tout cas dans les grandes organisations, que l'on ne peut pas échapper à l'articulation entre le contrôle permanent, la conformité et l'audit en termes de contrôle de dernier niveau.

La maîtrise du risque de non-conformité est certainement une figure imposée ; c'est un des risques sur lesquels le régulateur va être le plus vigilant, parce qu'il a des dimensions internationales qui peuvent affecter la réputation du secteur bancaire, les relations avec les régulateurs étrangers. Et parce que c'est un dispositif récent, il est normal que le régulateur se mette en position de l'auditer et d'apprécier comment les audits couvrent ce nouveau domaine de contrôle.

Nous devons nous attendre, dans le prolongement de la mise en place du 97-02, à ce que le régulateur fasse des missions sur ce thème-là.

Patrice JOSNIN

Je suis d'accord, c'est un thème effectivement récent, mais extrêmement important et il y a beaucoup plus qu'un enjeu réglementaire. Il y a pour nous un enjeu culturel. A l'occasion de nos audits, nous devons nous poser la question : quel est le degré de sensibilisation des équipes, du management, sur ces sujets de conformité dont le périmètre est immense ?

Louis VAURS

Une remarque. En définitive, le risque de non-conformité, c'est un point que tout service d'audit interne devrait vérifier très régulièrement, puisque le rôle de l'audit interne, c'est de s'assurer du bon fonctionnement du dispositif de contrôle interne. Or, un bon dispositif de contrôle interne doit permettre justement de s'assurer de la conformité aux lois et règlements. La seule différence, me semble-t-il, c'est l'importance donnée maintenant à ce thème et également la nécessité d'y mettre énormément plus de ressources qu'auparavant. Néanmoins, cela me paraît être l'une des bases et l'un des fondements mêmes de l'audit interne que de s'assurer qu'il y a un respect des lois et des règlements.

Michel LE MASSON

Pour un groupe international qui a différentes lignes d'activité dans différents pays, même s'il y a des thèmes communs, il est extrêmement difficile, notamment pour une équipe centrale d'inspection, de maîtriser tous les aspects réglementaires de tous les pays. En outre, la façon d'appréhender les sujets est très différente selon les pays. C'est pourquoi, le degré de maîtrise du risque de non-conformité se fera beaucoup sur des critères formels.
Evidemment, on peut contester cet aspect-là en disant : on ne regarde que la forme et finalement, on oublie le fond. Non. C'est à la fois un audit de forme et de fond, ce qui implique des moyens qui sont souvent démesurés, car cela nécessite de l'expertise sur la réglementation, cela nécessite de discipliner des organisations qui n'avaient pas l'habitude d'être normées de façon aussi forte ; et cela nécessite aussi une capacité à évaluer des situations extrêmement complexes. Un audit de conformité n'est pas un audit comptable, ni un audit de risque. La matière sous-jacente est plus complexe à appréhender.

Frédéric GEOFFROY

J'ajouterai que même si on a l'expertise dans la plupart des pays, on a en face de soi, quand on les contrôle, des équipes conformité qui ont au moins le même niveau d'expertise et qui ont la relation institutionnelle avec le régulateur, ce qui ajoute une difficulté supplémentaire.

Florence FRADIN

Je voudrais savoir si, dans le risque de non-conformité, vous englobez le risque de réputation ou est-ce que c'est un risque que vous cotez de façon spécifique ?

Michel LE MASSON

Le risque de réputation est plutôt une résultante du risque de non-conformité. Comme on l'a vu, être non conforme, cela peut prendre différentes formes. On peut ne pas respecter un règlement particulier très technique, très précis ; on peut ne pas être suffisamment vigilant dans les procédures d'ouverture de compte. En omettant de respecter la réglementation dans la forme, on se trouve face à un problème de fond majeur, qui se transforme en risque de réputation. Il y a des gradations dans le risque de non-conformité.
Le risque de réputation est la conséquence ultime d'un risque de non-conformité qui n'a pas été maîtrisé, dans un processus d'escalade lui-même non maîtrisé.

Patrice JOSNIN

Cette question est au cœur du sujet de la conformité, parce que c'est probablement le plus grand risque que courent les établissements. Le plus grand risque n'est pas d'avoir une amende de cent millions ou deux cents millions de dollars ; mais c'est l'image de

l'établissement à la suite de cette condamnation. Le risque en termes d'image est la chose que nous redoutons le plus, parce que nous ne savons pas le mesurer, ou très mal. Ne pas pouvoir appréhender ou mesurer la dimension d'un risque, c'est insupportable. Nous avons tous présents à l'esprit un certain nombre de grands établissements qui ont disparu en quelques semaines, voire en quelques jours, de grands établissements qui avaient près de cent ans d'existence, bien implantés dans le monde et qui, sur un problème de réputation, ont complètement disparu. Ils n'ont pas supporté le choc.

Claire VALTOT

Je voudrais juste donner un éclairage, qui est celui d'une banque internationale mais, j'allais dire, inversé.

J'ai le sentiment que le risque de réputation est extrêmement variable, et que les conséquences d'un même dysfonctionnement différeront totalement en fonction des pays.
L'impact que peut avoir une non-conformité, aux Etats-Unis ou au Japon, sur le risque de réputation, est probablement dix ou même cent fois supérieur à un dysfonctionnement identique dans un pays comme la France ou de l'Europe « latine » en général.
Cet élément-là fait qu'à mon sens il est plutôt imprudent de lier le risque de non-conformité et le risque de réputation de façon systématique. Il y a corrélation, il y a effectivement résultante, mais l'impact relatif n'est pas du tout le même selon les pays. J'aurais donc, sur ce point, une position un peu en retrait.

Michel LE MASSON

Souvent, le risque de non-conformité se transforme en risque de réputation parce que, pour des raisons culturelles, il y a une sous-estimation de la gravité de la non-conformité, et une non-conformité mineure dans le pays d'origine peut avoir une dimension tout autre dans un autre pays. Il y a cette dimension culturelle à intégrer.
Comme l'a dit Claire, il y a une différence d'appréciation des régulateurs sur un même sujet. La FED est beaucoup plus formelle et rigide que la FSA en Angleterre. Mais la FSA peut être aussi extrêmement brutale dans la façon d'appréhender certains sujets.
La seule solution, pour nous auditeurs internes, est de considérer ce sujet-là comme essentiel, d'aider nos directions générales à le prévenir en intégrant cette dimension dans nos plans d'audit, de telle sorte que nous ne soyons pas critiquables sur l'établissement de la cartographie des risques.
Le secteur bancaire est un métier qui repose sur la confiance. La confiance est liée à la conformité et à la réputation. Les enjeux sont donc beaucoup plus importants que dans n'importe quel autre secteur. Dans une société de surcroît très médiatisée, ces sujets doivent être traités avec attention. Cela devient une figure imposée incontournable.

Louis VAURS

Est-ce que votre souci majeur est le respect de la réglementation des pays étrangers ? Est-ce que le fait que la Commission bancaire se soit penchée très activement sur ce problème-là ne vient pas des difficultés qu'a pu avoir le Crédit lyonnais aux Etats-Unis, par exemple ? Ou est-ce complètement déconnecté ?

Michel LE MASSON

Il y a plusieurs réponses.
D'abord, l'ensemble des régulateurs communiquent entre eux : ils ont eux-mêmes une responsabilité de gouvernance du système financier à l'échelle mondiale, et il est normal qu'il y ait un dialogue de régulateur à régulateur.
Ensuite, il y a la mécanique, au moins au sein de l'Union européenne, de *home regulator* qui fait que c'est le régulateur du pays d'origine qui a la responsabilité globale de supervision sur base consolidée de l'établissement.
La Commission bancaire ayant une responsabilité de tutelle sur les groupes bancaires français, y compris dans leur extension internationale, si l'un de nos établissements a une difficulté avec un régulateur étranger, la Commission bancaire le saura parfois avant même que l'établissement ne le sache lui-même. Il n'y a pas de problème de conformité qui puisse intervenir dans un pays proche de nous sans que la Commission bancaire en soit informée, parce qu'il n'y a pas d'étanchéité entre les différents régulateurs sur ces sujets-là.

Frédéric GEOFFROY

Je dirai aussi qu'il y a de moins en moins d'étanchéité dans les transactions. Un produit fabriqué en France, peut être vendu par une équipe opérant à Londres, à un client espagnol ou d'un autre pays européen, et le *booking* se fera à Paris ou à Londres. On est donc obligé de prendre en compte l'ensemble des dispositifs de conformité.

Patrice JOSNIN

On a beaucoup parlé des régulateurs, mais la conformité concerne également d'autres entités. Ainsi l'OFAC (Office of Foreign Assets Control – USA) établit les listes de personnes morales et physiques avec lesquelles on ne doit pas traiter la moindre opération.

Question dans la salle

Comment, à travers vos audits de conformité, intégrez-vous le risque commercial qui pourrait naître d'asymétries réglementaires entre la France et des pays dans lesquels il y aurait des succursales ou des filiales ; la France, de par l'application d'une réglementation plus « disante », faisant naître un risque commercial important ?

Patrice JOSNIN

Pour ce qui concerne notre établissement, nous appliquons toujours la règle du mieux-disant, c'est-à-dire du plus sévère. C'est vrai que l'on ne se fait pas toujours des amis des commerciaux. L'auditeur, comme le *compliance officer*, va souvent à l'encontre de l'intérêt commercial immédiat.

Question dans la salle

S'agissant du risque de non-conformité et du risque juridique, le spectre de la fraude n'est jamais très loin. Qu'il s'agisse de la fraude d'un individu malveillant ou d'une fraude plus institutionnalisée, comme la publication de fausses informations financières, quels sont les dispositifs que vous avez mis en place pour évaluer le climat général éthique et déontologique, qui est par ailleurs une exigence des normes de l'IIA/IFACI ?

Michel LE MASSON

Votre question comporte plusieurs éléments.
La fraude n'est pas le risque de non-conformité ; elle fait partie de notre champ d'investigation traditionnel. C'est un sujet un peu à part.
La question que vous soulevez est plus d'ordre managérial et culturel, parce qu'au fond la prévention du risque de non-conformité est directement liée aux valeurs que l'entreprise met en avant, aux valeurs inculquées – si je peux me permettre cette expression – par le management. Le risque de non-conformité, pour une organisation, c'est qu'un comportement individuel d'un collaborateur puisse mettre en risque l'ensemble de cette organisation, soit de façon involontaire, par manque de professionnalisme, soit de façon intentionnelle (délit d'initié par exemple).
Il faut donc une éthique. L'éthique fait partie des valeurs de l'entreprise, et il appartient au management de le réaffirmer via nos missions d'audit, c'est-à-dire en y attachant l'importance et la gravité voulues. Si je vous ai dit que, de mon point de vue, les recommandations afférentes à la conformité sont des recommandations de niveau élevé pour l'organisation, c'est bien pour appréhender cette dimension-là.
On débouche, après la partie éthique, sur la partie managériale : quelle est la capacité des collaborateurs à anticiper ou à gérer le risque de non-conformité ?
Il y a des secteurs dans la banque où l'on intègre cette donnée dans l'évaluation des collaborateurs, et dans leur rémunération. Un comportement qui met l'établissement en risque de non-conformité peut être sanctionné selon différentes gradations.
A l'étranger, les régulateurs évaluent et apprécient la façon dont sont notés les collaborateurs. Il me semble que la Commission bancaire a la même vision des choses aujourd'hui.

Claire VALTOT

Je voudrais juste revenir sur la conclusion initiale de Michel Le Masson, qui était de conforter l'audit dans le contrôle de dernier niveau, le régulateur ayant renforcé l'échelon intermédiaire de contrôle permanent.
Ma question s'adresse à la salle. J'aurais voulu savoir, à main levée, quels sont ceux chez qui le contrôle permanent et la conformité sont séparés.
Cela représente environ 2/3 de la salle.
Pensez-vous que le contrôle permanent de la conformité est fait par les départements de contrôle permanent ? Ou pensez-vous que l'audit fait ce travail ?

Une participante dans la salle

C'est sûrement une excellente question, Claire, parce que dans les faits la Commission bancaire pose la même question. Elle nous a demandé, récemment, si le contrôle permanent était en charge du contrôle de la conformité.

Donc combien, dans la salle, sont convaincus que le contrôle permanent vérifie la conformité ?

Claire VALTOT

Ce que je comprends, c'est qu'aujourd'hui on a bien instauré un dispositif de conformité, de contrôle de la conformité. On a, à côté, un dispositif de contrôle permanent, mais le contrôle permanent ne contrôle pas ce que fait notre département conformité.
Il faut donc bien insister sur la conclusion de Michel qui consiste à dire : l'audit doit effectivement être le dernier niveau, c'est-à-dire celui qui s'assure que tout cela fonctionne bien.

Aujourd'hui, nous ne sommes pas sûrs, nous auditeurs internes, que cette étape de contrôle est effective. Notre prochain défi est de s'assurer que le contrôle permanent met en œuvre un dispositif de contrôle de ce que fait la conformité.

Patrice JOSNIN

Je ne pense pas que l'on puisse clore ce sujet. La façon dont j'aurais tendance à l'aborder, c'est de dire : la conformité est une fonction de contrôle, une des composantes du contrôle interne. C'est un sous-ensemble de l'ensemble Contrôle permanent.
A ce titre, de mon point de vue, c'est au contrôle périodique de contrôler la conformité. Mais vous avez le droit d'avoir un point de vue différent.

Claire VALTOT

Je pense que le rôle de la conformité est très variable selon les établissements, et que, de ce fait, il n'y a pas de réponse universelle.

Michel LE MASSON

Je voudrais apporter un complément en expérience internationale.

La conformité, il y a dix ans, était entre les mains des juristes qui commentaient la réglementation et la législation et s'assuraient qu'elles étaient respectées.
Aujourd'hui, la conformité ne consiste plus à commenter la réglementation et à donner des avis. La fonction est devenue opérationnelle : les officiers de conformité, ceux qui font de la *compliance*, connaissent les systèmes, connaissent les produits. Ils doivent être capables d'analyser les systèmes, de les exploiter, et de faire un certain nombre de contrôles en amont, faute de quoi le dispositif est inopérant.
Le premier niveau de contrôle permanent doit être exercé par les membres de la conformité eux-mêmes.
Il y a ensuite un contrôle permanent de deuxième niveau qui prend un peu plus de recul. Il fait des sondages et s'assure, dans le domaine de la conformité, que les contrôles sont bien en place.
Il y a enfin l'audit, contrôle de dernier niveau, qui s'assure que toute la chaîne fonctionne.
Il m'est arrivé de faire des missions d'audit sur des thèmes de conformité sur lesquels la conformité n'était pas intervenue, et à l'époque, il n'existait pas de structure de contrôle permanent. L'audit mettait au jour des anomalies qui ne relevaient pas, de mon point de vue, d'une fonction d'audit telle qu'on l'entend aujourd'hui, et qui auraient dû être filtrées par un niveau de contrôle préliminaire.
Le régulateur, en mettant en place ce dispositif, a anticipé le fait que, dans des organisations importantes et complexes, on ne peut pas se reposer uniquement sur des corps d'audit et d'inspection qui font du contrôle périodique.

Question dans la salle

On n'a pas parlé de la fonction contrôle des services d'investissement. Le règlement général de l'AMF prévoit notamment qu'il y a une partie de conseil chez le nouveau RCSI. Le « C » ne veut plus dire « contrôle », mais « conformité ». De nouveaux articles du règlement général de l'AMF précisent bien un rôle de conseil tout à fait en amont. Il ne s'agirait donc plus de contrôle ?

Michel LE MASSON

Il s'agit de contrôle pour partie. La fonction de conseil fait partie de la fonction opérationnelle, mais pour autant la notion de contrôle n'est pas absente. Même un commercial du *front office* doit faire du contrôle. Le contrôle n'est pas saucissonné. Le fait qu'il existe des corps de contrôle dédiés, ne supprime pas l'obligation pour tous les membres de l'organisation de s'approprier le contrôle.

Question dans la salle

Vous représentez des banques importantes ou très importantes. Dans les établissements plus modestes, certaines fonctions, comme celles de RCSI, blanchiment, etc., sont assurées par les contrôleurs permanents, voire périodiques. D'où la grande difficulté du positionnement du directeur de la conformité.

Michel LE MASSON

C'est vrai. L'époque où une inspection générale s'occupait à la fois de conformité, de contrôle, de fraude, de prévention, etc., n'est pas si lointaine, y compris dans les grands établissements. Il est normal que cette organisation, qui se met en place d'abord dans les grands établissements, soit compliquée et nécessite un temps de rodage, période qui sera plus longue encore pour les établissements de taille intermédiaire.
Le régulateur fait preuve de pragmatisme et admet que certaines fonctions (contrôle permanent et conformité) puissent être réunies dans de plus petits établissements. On ne peut pas imposer à tous la même structure d'organisation et de coûts.

Claire VALTOT

On observe en effet que les départements de conformité – on peut classer les RCSI et les RCCI dans cette catégorie-là – ont la double fonction de contrôleurs de premier niveau (c'est-à-dire de personnes qui, dans l'organisation, donnent un avis et s'autocontrôlent), et de contrôleurs de deuxième niveau (c'est-à-dire qu'ils contrôlent l'existence d'un contrôle sur d'autres opérations). C'est bien la difficulté que l'on rencontre avec les départements de conformité qui sont très fréquemment, y compris dans les grands établissements, des deux côtés de la barrière à la fois, et c'est ce qui soulève la question subsidiaire : qui contrôle la conformité quand elle est en premier niveau ?
Il n'y a pas de bonne réponse. Chaque département de conformité ayant une liste d'opérations de premier niveau, si je puis dire, qui lui est propre, on ne peut pas donner la liste de ce qu'il y a à faire ou à ne pas faire. Mais cette question-là, elle existe et le curseur étant positionné, chez les uns et chez les autres, de façon totalement différente parce que c'est un problème de volumes, de nombre d'employés, d'organisation, il n'y a pas de réponse unique. Et cette question-là, de savoir qui contrôle qui et quoi, évidemment l'auditeur doit se la poser, parce qu'effectivement, comme le rappelle Michel, la conformité fait partie du contrôle permanent, et dans un certain nombre de cas, on risque effectivement de mélanger les genres. Pour certaines opérations très spécifiques, je ne pense pas que ce soit un problème, l'essentiel étant que, dans ces cas-là, notre plan d'audit intègre cette dimension.

Patrice JOSNIN

Abordons maintenant le troisième thème, la MIFID.

- 1993 : directive des services d'investissement.
- 1996 : transposition en droit français de cette directive.
- 2004 : remplacement de cette directive.
- Septembre 2006 : une nouvelle directive et un règlement.

La directive européenne MIF a été transposée ; s'en est suivie une cascade de textes : une loi du 20 février 2007 autorisant le gouvernement à prendre une ordonnance pour transposer la directive européenne ; une ordonnance prise au mois d'avril 2007 ; le règlement général de l'AMF, homologué par un arrêté le 15 mai 2007. Un certain nombre de textes et d'arrêtés sont en préparation ; ils sont au nombre de cinq, dont un, d'ailleurs, va porter modification du règlement 97-02. Tous ces textes sont appelés à entrer en vigueur le 1er novembre 2007.

Frédéric GEOFFROY

L'entrée en vigueur de la directive sur les marchés d'instruments financiers est effectivement prévue pour le 1er novembre 2007. Ce n'est donc pas encore vraiment une figure imposée.
Il n'y a pas à proprement parler de jurisprudence, et le retour d'expérience pour chacun d'entre nous doit être assez mince puisque nous n'avons pas eu l'occasion de contrôler l'application des dispositions de la directive MIF.
Ceci étant, comme l'a expliqué Patrice, un certain nombre de textes ont été adoptés, transposant dans la réglementation française les arrêtés et décrets du 15 mai. Chacun de nos établissements a lancé un certain nombre de projets.
Les équipes travaillent généralement depuis au moins un an sur l'application de la MIF. C'est le sujet d'actualité. L'impact de ce projet est très important pour l'ensemble des établissements.
Tout n'est pas définitivement arrêté. Patrice a parlé de l'adaptation du 97-02. Il y a également, entre les différents régulateurs nationaux (notamment entre l'AMF et la FSA, concernant par exemple la *best execution policy* ou les opérations *cross-border*), un certain nombre de dispositions qui mériteraient d'être clarifiées.

De manière très générale, quels sont les grands changements ? C'est d'abord une formalisation accrue et des exigences organisationnelles. Là où, auparavant, on avait essentiellement des règles de conduite, on a, pour beaucoup, des exigences organisationnelles, et donc un risque réglementaire accru.
Les conditions dans lesquelles les relations clients sont gérées passent au premier plan. Le risque de réputation et le risque d'image deviennent prépondérants et l'audit intervient en prévention de ces risques.
Pour illustrer ces exigences organisationnelles, je vais vous citer l'article ancien et le nouvel article sur le conflit d'intérêts. L'article ancien disait : « Les PSI doivent s'efforcer d'éviter les conflits d'intérêts et, lorsque ces derniers ne peuvent être évités, veiller à ce que leurs clients soient traités équitablement. » Le nouvel article dit : « Les PSI doivent prendre toutes les mesures raisonnables [influence des textes anglo-saxons] pour empêcher les conflits d'intérêts de porter atteinte aux intérêts de leurs clients. Lorsque ces mesures ne suffisent pas à garantir que le risque de porter atteinte aux intérêts des clients sera évité, le prestataire informe ceux-ci. »
Il faut définir une charte globale pour les établissements présents dans plusieurs pays ; une charte qui concerne l'ensemble du dispositif. Il faut définir des scénarios, identifier, enregistrer les conflits d'intérêts. Il faut définir une politique de gestion de conflits d'intérêts. Enfin il faut informer précisément les clients, et il est à prévoir que les clients reviendront très largement sur cette obligation d'informer.

Je ne vais pas entrer dans le détail des changements, mais j'en citerai simplement deux qui paraissent également majeurs. Premièrement, des règles de conduite fondées sur une différenciation marquée des régimes de protection applicables selon la nature du client (vous connaissez la distinction client professionnel, contrepartie éligible, client de détail).
Là, on va beaucoup plus loin que ce qui a été fait dans la plupart des établissements, avec un travail de documentation de la relation clients qui sera centralisé, à la Société générale, dans un back-office unique, une information formelle du client, un archivage de données clients, et donc des procédures, des mesures très précises, une organisation, ce qui va nous faciliter, d'une certaine façon, le travail d'audit de tout ce dispositif, mais ce qui constitue également un travail très important pour SGIB. Pour la BFI de la Société générale, ce sont 15 000 clients, 3 000 éligibles et une bonne partie de ces clients partagés entre plusieurs lignes métier.
Deuxièmement, le principe de meilleure exécution des ordres du client, l'obligation de mettre en place une *policy*, des *reportings*, des exigences renouvelées en matière d'archivage, des exigences étendues à cinq ans, avec l'obligation d'informer le client et de conserver ces informations sur des supports durables.
Tout cela, ce sont des sujets très précis qu'il nous faudra auditer demain et qui sont beaucoup plus formalisés, beaucoup plus cadrés que ce que l'on avait l'habitude de voir. Mais ce sont des sujets que l'on avait aussi assez largement abordés, sous un angle ou sous un autre, même si la gestion de la relation clients n'était pas forcément ce que l'on avait en tête de liste dans notre plan d'audit. Mais l'on ne passe pas directement d'une espèce de no man's land à un ensemble de figures imposées. Il y avait quand même un certain nombre de figures libres – je crois que Claire va en parler – qui reprenaient ce que nous allons devoir faire demain pour contrôler le respect de ces dispositions.

Pour l'audit, beaucoup plus concrètement, il y a sept étapes.

- La première, c'est évidemment le suivi du projet. Les projets ont démarré depuis un an. L'information clients va se faire en août ou septembre, selon les établissements. Nous devons être prêts pour novembre. Nous avons un rôle de monitoring et d'alerte en ce qui concerne le projet qui, encore une fois, est un projet très lourd.
- La seconde étape est évidemment la formation des auditeurs. On a commencé et l'on doit être prêt en fin d'année pour les premières missions que l'on va vraiment lancer sur ce thème.
- En parallèle, on va débuter le *risk assessment*. On avait déjà une catégorie Bâle II, la première, que l'on avait intégrée dans notre outil de *risk assessment*, qui reprenait en fait l'essentiel des dispositions Bâle II. Concernant l'outil, il y a peu de choses à modifier mais, là encore, l'orientation est beaucoup plus accentuée sur tout ce qui est gestion de la relation clientèle, identification des risques.
- On est *risk assessment* entité, on n'est pas *risk assessment* processus, mais c'est quand même quelque chose que l'on va devoir prendre en compte, ne serait-ce que pour prévoir un certain nombre de missions thématiques. C'est la quatrième étape.
- Une mission est prévue en fin d'année 2007 : bilan du projet, bilan de la mise en place de la MIF.
- En 2008, ce seront des missions thématiques sur un certain nombre de thématiques MIFID, des missions tests essentiellement sur des *front offices*, des équipes de vente, qui nous permettront de définir le corps de méthodologie qui sera ensuite déroulé par les auditeurs. C'est la sixième étape.
- La septième étape sera, en fin d'année 2008, une mission de suivi des recommandations qui auront été faites dans le cadre de la mission de vérification du projet, et une synthèse qui sera à la disposition des régulateurs.

C'est un cadre bien normé, une exigence de formalisation des procédures qui devrait faciliter l'intervention de l'audit, et un plan que nous allons devoir dérouler sur 2008.

Claire VALTOT

En synthèse, par rapport à ce que vient de vous exposer Frédéric – et je pense que vous aurez des questions sur le déroulement de tout ce processus en interne et son inclusion dans le processus général de l'entreprise – la question que l'on peut se poser est : est-ce réellement quelque chose de nouveau ? Auparavant, on faisait déjà des audits de conformité. Est-ce une nouvelle figure imposée ? Ma réponse, qui n'engage que moi, est probablement négative. Néanmoins, on est en face d'un changement réglementaire très profond, qui impacte la quasi-totalité des activités de l'entreprise – puisque la question des conflits d'intérêts se pose tant dans la banque *retail* que dans l'*asset management*, et la banque d'investissements – pour lesquelles la connaissance générale, la diffusion de l'information n'est pas forcément très étendue au sein de l'entreprise. Notre rôle est de nous assurer que tout le monde suit bien la démarche en temps et en heure.
Les risques sont accrus pour l'entreprise, parce que les systèmes ne sont pas forcément à jour, parce qu'ils ne sont pas toujours capables de traiter la question, notamment de la *best execution*, du mode de contrôle, de la gestion.
La question du contrôle de conformité, par rapport à toutes ces exigences nouvelles, se pose dans un calendrier très court, puisque la directive a été déclinée en mai et qu'elle est d'application au 1er novembre. Nous avons six mois pour travailler, ce qui est très peu. Face à cette urgence, nous nous devons d'être réactifs.

Un certain nombre de questions sensibles restent ouvertes, notamment dans les groupes internationaux, comme celle-ci : que faire quand la directive a été déclinée dans notre pays et qu'elle n'a pas été déclinée ailleurs ?
Il existe une déconnexion des enjeux réglementaires, certes temporaire mais encore d'actualité, sur laquelle, nous auditeurs dans les groupes internationaux, devons être très vigilants, parce que les exigences des uns ne seront pas les exigences des autres. On parlait tout à l'heure du risque commercial, on est exactement dans ce cas-là.
Dans le domaine des conflits d'intérêts, l'audit aide, contribue à défricher le terrain. On se rend compte que l'activité bancaire est une mine de conflits d'intérêts. Jusqu'à présent, on vivait assez bien avec cela. Mais aujourd'hui, non seulement il faut vivre avec cela, mais il faut le normer, le documenter, tenir des registres qui recensent les situations potentielles de conflits d'intérêts et qui expliquent comment on les gère, savoir comment informer le client, s'interdire de procéder à certaines opérations qui semblaient fort bénignes antérieurement. C'est un deuxième enjeu sur lequel il y a beaucoup de travaux réalisés aujourd'hui chez ABN-AMRO, mais j'imagine que dans tous les autres établissements, il y a ce type travaux auxquels l'audit peut contribuer avec efficacité.
Il y a également tout ce qui touche aux prestations externalisées. Dans le cadre de la *best execution*, on peut choisir de traiter avec un certain broker sélectionné pour sa capacité à délivrer un bon service à un prix intéressant, lequel broker délèguera son dépouillement à un tiers. Comment faire pour s'assurer que cette *best execution* et la prestation qui en découle, éventuellement externalisée, entre dans le cadre de la MIF ? Quel dispositif de contrôle et, partant, d'audit dois-je mettre en œuvre ? Ces questions commencent à se profiler à l'horizon, et l'on aura certainement à les analyser dans la période 2007-2008.

Patrice JOSNIN

J'aimerais savoir si vous avez envisagé, un peu à l'instar de ce que l'on a fait pour Bâle II, de faire une mission intermédiaire pour savoir où en est le projet pour répondre aux exigences du MIFID. Est-ce que l'audit va, avant le 1er novembre, dire : « Voilà notre degré de préparation (ou d'impréparation) par rapport à ce que l'on va nous demander. » ? Prévoyez-vous ce type d'audit ou pas ? Ou bien vous dites-vous : « Tous les textes ne sont pas sortis. Attendons 2008. » ? Quelle est votre position ?

Frédéric GEOFFROY

Nous assurons un monitoring du projet et adressons des comptes rendus réguliers à la direction, mais il s'agit plutôt d'un rôle d'alerte que d'une mission. La mission proprement dite, sur la mise en place du projet, est prévue pour la fin de l'année.

Florence FRADIN

Je voudrais savoir si des compétences spécifiques sont requises dans le cadre de l'audit de la MIF. S'agissant d'un processus complet, a-t-on besoin d'une équipe multidisciplinaire ? Avez-vous prévu, planifié ou réfléchi à l'équipe idoine ?

Claire VALTOT

Il y a parmi mes auditeurs un détenteur de la carte de RCSI, qui connaît bien notamment le règlement général de l'AMF. Il y a deux membres de l'ACAMS, donc particulièrement compétents sur *compliance* et *anti-money laundering.*
On parle là d'un sujet qui tourne beaucoup autour du règlement général de l'AMF. Je pense qu'il faut avoir des compétences dans le domaine, si l'on veut s'engager dans un audit de conformité ou d'avancement de conformité concernant une directive MIF. Mais c'est une opinion qui n'engage que moi.

Frédéric GEOFFROY

Je ne prévois pas de constituer une équipe dédiée au contrôle de la MIF. Des actions de formation vont être entreprises. Le sujet est complexe, mais il ne l'est pas autant que, par exemple, le contrôle des modèles dont on parlait tout à l'heure.

Patrice JOSNIN

Le quatrième exercice obligé qui s'impose à l'audit concerne les activités externalisées. C'est un thème qui a mobilisé beaucoup de monde et de nombreux groupes ont travaillé sur le sujet de l'audit de ces activités : la FBF ; le groupe Robustesse, managé par la Banque de France, auquel participe le Trésor et un certain nombre d'établissements de la Place ; un groupe de travail dit du G7, qui regroupe sept établissements bancaires de la Place ; et puis, il y a l'IFACI. Le groupe Banque de l'IFACI a travaillé sur la question. Un sous-groupe animé par Frédéric Geoffroy, auquel a participé Claire Valtot, a publié un cahier de recherche sur l'audit des activités externalisées.

Claire VALTOT

La question sur les activités externalisées se pose depuis la publication du règlement 97-02 modifié en mars 2005, et qui était d'application au 1er janvier 2006. Ce règlement a créé une espèce de tsunami dans les établissements bancaires, qui portait essentiellement sur deux problématiques.
Première problématique, d'ordre contractuel. L'externalisation des prestations a impliqué une révision intégrale des contrats, et une mise au point des conditions d'accès à l'information chez le prestataire sachant que, auparavant, ces prestations de service étaient régies par la loi sur la sous-traitance, qui date des années 1970.
Deuxième problématique : il a fallu se poser des questions sur ce qu'était l'externalisation. Est-ce qu'on avait externalisé une prestation dite essentielle ou non ? Comment organisait-on le contrôle autour de cette activité-là ? En cette matière, je dois dire que le cahier de recherche de l'IFACI sur les prestations externalisées donne des clés d'analyse extrêmement utiles, voire essentielles, et je vous engage vivement à vous le procurer si vous ne l'avez déjà fait.

Dans la mise en œuvre des activités externalisées, il y a en gros deux phases. La première s'étendait en théorie jusqu'au 1er janvier 2006, date d'application du règlement, et qui concernait la revue du dispositif par l'organisation, l'identification des processus externalisés, le mode de fonctionnement : les contrats de sous-traitance étaient-ils adaptés compte tenu des nouvelles exigences réglementaires ? Des systèmes de contrôle avaient-ils été mis en place autour de ces contrats ? Existait-il des indicateurs de performance, des clauses d'audit, des clauses de suite ?
Cette phase est donc théoriquement achevée depuis le 1er janvier 2006. Sachez que ce n'est pas toujours le cas, notamment pour des prestations lourdes et essentielles sur lesquelles le G7 réfléchit activement.
L'audit peut intervenir dans cette phase, pour épauler le dispositif, donner des clés d'analyse, s'assurer que la méthodologie adoptée est exhaustive, que tous les aspects sont couverts.
Une fois ce travail d'identification effectué, comment définit-on une stratégie d'audit et de contrôle permanent au regard de ces prestations de service externalisées ? La stratégie d'audit (c'est-à-dire l'inclusion dans le plan d'audit, le *risk assessment* et la méthodologie d'audit que l'on va déployer au regard des activités externalisées), est encore chez moi – je suis peut-être très en retard – au stade de la réflexion. Nous avions l'idée d'intervenir chez certains prestataires. Peut-on réellement le faire, est-ce que cela fait sens, est-ce que l'on ne va pas débarquer chez notre prestataire en même temps que dix autres établissements bancaires ? Est-il logique d'intervenir de façon décorrélée ? Et si l'on intervient de façon coordonnée, comment structurer l'affaire ? Fait-on appel à des prestataires extérieurs, encore une fois? Ou mandate-t-on l'un d'entre nous pour le faire pour compte commun ? Cette dernière éventualité rencontre l'adhésion de l'OCBF, entre autres.
D'autres démarches sont en cours de réflexion, comme la création d'une sorte de GIE qui éviterait les démarches unitaires.
La stratégie d'audit que l'on doit déployer vis-à-vis de nos prestations externalisées, est, pour moi, encore une fois, dans une phase de gestation ; ce qui n'empêche pas que, en parallèle, aient été définies, pour certaines prestations, des démarches individuelles qu'on accomplit, comme on l'a toujours fait auparavant.
Voilà pour la phase de lancement.

La deuxième phase est le régime de croisière : il y aura un *risk assessment*, une stratégie d'audit, un plan d'audit pour l'ensemble de nos activités externalisées ; on adoptera éventuellement une démarche conjointe avec plusieurs établissements ou on sous-traitera à un tiers prestataire d'audit, ce qui est envisageable.
La question est : que va-t-on vérifier ? On va vérifier tout ce qui concerne l'organisation des contrôles chez le prestataire ; l'existence de conventions d'externalisation que l'on aura définies ; les indicateurs de performance, leur nature, leur mode de contrôle, leur communication, leur pertinence, leur nombre (suffisant ou non), etc.
Comment s'assure-t-on que notre prestataire respecte notre réglementation, puisque l'on a inventé, par le biais de ce règlement, la transfrontalité, si je puis dire, des règlements, y compris chez nos prestataires étrangers. Il y a, là aussi, tout un enjeu en matière de méthodologie d'audit, tout à fait important et sur lequel il faut que l'on travaille, encore une fois, chacun avec ses normes, et en fonction des règles et lois qui lui sont applicables. En ce qui me concerne, en tant qu'établissement d'obédience hollandaise, je dois respecter un set de lois et règlements hollandais, français et américains, parce que je suis cotée aux Etats-Unis. C'est tout un environnement qu'il convient d'intégrer.
Et puis, comme toujours, on regarde ce qui existe, mais il faut aussi regarder ce qui n'existe pas. L'expérience très récente m'amène à penser que, chaque fois que l'on soulève une pierre, en ce moment, on trouve un contrat d'externalisation. Et parfois, on peut se poser la question de la prestation de service essentielle sur certains contrats : prestations informatiques, prestations concernant la production comptable ou touchant à des questions de détermination des enjeux en termes de risque, etc. On voit bien que le périmètre est

mouvant et que, au fur et à mesure des audits que l'on va mener, on sera de plus en plus souvent amené à étendre notre analyse.
La conclusion que je tirerai par rapport à la phase de lancement et au régime de croisière est qu'il y a un certain nombre d'étapes obligées qu'il convient aujourd'hui de mettre en œuvre. On se rend alors bien compte que la méthodologie est en cours de définition.

Une conséquence concrète de l'externalisation, aujourd'hui, est l'extension du champ du contrôle hors des frontières de l'entreprise. C'est quelque chose de tout à fait nouveau qui pose la question de la responsabilité. Quelle est la responsabilité réelle de la banque quand notre prestataire ne remplit pas ses obligations réglementaires ? Peut-elle être tenue pour responsable d'un fait qui lui est étranger ?
Supposez que votre prestataire de service Titres, qui fait la tenue de comptes Conservation pour vous, manque à une obligation réglementaire. Vous l'identifiez. Que faites-vous, sachant que pour sortir d'un contrat de prestation de service de cet ordre, il faut de six mois à un an ?
Se pose aussi la question de la capacité à intervenir chez le prestataire : peut-on, ne peut-on pas ? Pouvons-nous réellement faire des travaux de qualité dans cet environnement-là ? Question subsidiaire : si nous pouvons intervenir, quelle suite sera donnée à notre intervention ? Comment nos prestataires prendront-ils en compte nos recommandations ?
Pour moi, ce sont les deux questions ouvertes, aujourd'hui, dans ce domaine.

Frédéric GEOFFROY

Je ferai deux remarques. La première c'est que je suis frappé par la grande convergence des différentes réglementations nationales. La deuxième, c'est que l'externalisation est d'abord une responsabilité des opérationnels : les procédures de surveillance permanente doivent inclure le contrôle des activités externalisées, ce qui n'est pas toujours le cas. L'audit, le contrôle périodique, intervient en second niveau.
Nous avons commencé à faire un certain nombre de missions, dans le groupe. Nous avions d'ailleurs commencé avant la réglementation, puisqu'il existait déjà un certain nombre de clauses d'audit dans les contrats négociés. Nous avons une certaine expérience dans le domaine.
Le seul point d'interrogation concerne effectivement la communication avec le prestataire, le suivi de la mission, les recommandations. Sans aller jusqu'à la responsabilité juridique du service d'audit de la banque qui fait la vérification, il est vrai que c'est en fin d'audit que l'on peut rencontrer un certain nombre de difficultés.
Notre stratégie maintenant, c'est de se donner des objectifs, sur les trois ans qui viennent, pour couvrir complètement toutes les activités externalisées.

Patrice JOSNIN

Je voudrais rappeler un point que nous devons tous avoir bien présent à l'esprit, c'est que l'externalisation n'ôte en aucun cas la responsabilité du délégant concernant la prestation externalisée. C'est un principe intangible.
L'audit des prestations externalisées nous amènera à toujours repousser les lignes, pour employer un langage politique, jusqu'au risque fournisseurs, et des fournisseurs qui sont totalement critiques. C'est une donnée que l'on doit prendre en compte, qui doit entrer dans le champ de l'audit.
Autre remarque : quand on va auditer chez le prestataire externalisé, il faut veiller à bien limiter son audit à l'objet de la prestation et ne pas s'ingérer dans les affaires du prestataire.

Question dans la salle

Jusqu'à quel point peut-on se reposer ou utiliser les travaux de l'audit interne du prestataire ?

Patrice JOSNIN

La question est intéressante. Lorsqu'un prestataire a un audit très mature, doit-on à nouveau, nous, en tant que délégant, conduire un autre audit ?
Je crois que la réponse est oui, quand il s'agit d'un prestataire non bancaire. Quand il s'agit d'un prestataire bancaire, c'est différent.
Comme l'ont dit Claire et Frédéric, il y a deux aspects dans l'audit à conduire.
Il y a audit chez le délégant, d'abord : sur les conditions d'attribution du marché, l'appel d'offres, l'établissement du contrat, la personne en charge de la relation, l'implication du contrôle permanent…
Et il y a l'audit chez le délégataire, pour s'assurer notamment qu'il n'a pas subdélégué.

Un participant dans la salle

Je voulais faire un retour d'expérience, pour aller tout à fait dans votre sens puisque, en ce qui nous concerne, nous avons plutôt intégré des audits de prestataires dans le cadre d'audits de processus. Je n'ai pas encore, à l'heure actuelle, pratiqué d'audit de prestataire « sec ».
Dans le processus traitement des chèques ou traitement des espèces, par exemple, on traite effectivement dans la banque la totalité du processus ; on termine par l'examen – comme vous venez de le dire – des contrats, de ce que fait le contrôle permanent, de ce que font aussi les opérationnels dans le cadre du contrat qualité, par exemple, du suivi du prestataire.
Il me semble qu'au-delà des obligations réglementaires, il est intéressant d'intégrer ce genre d'audit dans des processus.
Je voudrais faire une remarque sur la mutualisation. Je pense que, dans la même optique de traitement des processus, il me paraît assez difficile de mandater l'un d'entre nous pour faire des audits car beaucoup de processus sont propres à la banque ; il est donc peut-être préférable de faire appel à des audits externes. Mais cela n'engage que moi et pas mon établissement.

Patrice JOSNIN

C'est tout à fait la préconisation du groupe de travail G7.

Claire VALTOT

Nous sommes intervenus dans le passé pour compte commun d'un groupe de deux banques dont nous faisons partie et qui avaient des intérêts très similaires auprès d'un prestataire. Nous ne sommes pas les seuls à travailler avec ce prestataire. Il s'est trouvé que l'on a « consortialisé », si je puis dire, nos besoins. Cela s'est très bien passé, nous avons travaillé de façon très ouverte avec notre partenaire.
Je pense que c'est une question propre à chacun. L'avantage que je vois à passer par un tiers, c'est que ce tiers est neutre. En général les banques externalisent le plus souvent dans d'autres banques.
Quand on envoie notre département d'audit chez un confrère, il le vit plutôt mal, soit parce que son département d'audit est mature, soit parce qu'il pense que l'on vient faire de l'espionnage industriel, ou qu'on est le cinquième d'une longue série.
Je pense que le fait de passer par des tiers, c'est l'avenir, et que l'on arrivera assez rapidement à structurer une démarche de place autour de ces problématiques. Mais encore faut-il que le prestataire soit d'accord.

Question dans la salle

J'ai une question sur les prestations externalisées, concernant la prise en compte d'un rapport de type SAS 70, qui existe dans l'univers SOX. Avez-vous déjà été confrontés à la présentation de ce type de rapport ? Peut-il intervenir de façon palliative à un audit chez un prestataire externalisé ?

Claire VALTOT

Oui. On m'a déjà présenté des SAS 70. Je les ai déjà utilisés. La seule chose que j'ai faite – cela m'est arrivé une fois – c'est de demander des tests complémentaires à SAS 70.
Il se trouve que le groupe ABN-AMRO a sous-traité son informatique, notamment la production informatique auprès d'un externalisateur classique qui est IBM. IBM, pour éviter que tous ses clients exactement les mêmes tests à deux jours d'intervalle, produit des SAS 70.
Le SAS 70 que l'on m'a donné était tout à fait complet, sauf qu'il n'y avait aucun test sur la France. On a donc demandé que des tests complémentaires soient effectués pour la France, de façon à garantir une couverture de nos activités.
La démarche est bonne à condition de faire ce que l'on ferait dans n'importe quel cas, à savoir de s'assurer que la démarche d'audit qui a été suivie ou les contrôles clés qui ont été testés dans le SAS 70 sont les mêmes que les nôtres.
En général, les SAS 70 sont élaborés par des professionnels qui ont une grosse expérience du sujet. Donc le risque est plutôt faible. Il faut seulement s'assurer que le périmètre de tests comprend bien l'ensemble de nos activités.
On peut ergoter sur le fait qu'un SAS 70 est une norme américaine et non pas une norme européenne. Mais il existe une IFRS qui fait le même usage et qui globalement aboutit au même rapport.

Patrice JOSNIN

Nous abordons maintenant notre dernière figure obligée, le PCA (plan de continuité d'activité) ou BCP (*business continuity plan*).
La continuité est un sujet avec lequel nous sommes tous très familiarisés, depuis longtemps, dans le domaine de l'informatique (procédures de *backup*).
Le PCA couvre l'intégralité des activités stratégiques de la banque. C'est, je crois, une préoccupation assez nouvelle. Et ce qui est encore plus nouveau, c'est de l'avoir introduite dans notre règlement 97-02 du 31 mars 2005, avec l'obligation d'auditer le PCA, et notamment de s'assurer qu'on le teste.

Claire VALTOT

Le PCA, c'est le plan de continuité d'activité générale de la banque.

Le plan de secours informatique est un sujet normé, implanté et industrialisé, et qui existe dans la réglementation depuis une dizaine d'années environ.
Le plan de continuité d'activité concerne l'ensemble des activités, ou au moins les activités critiques. La Commission bancaire, aujourd'hui, demande à chaque établissement bancaire d'avoir un PCA.

Que devons-nous faire, nous, auditeurs, pour s'assurer que le PCA fonctionne bien ?
De deux choses l'une, ou il existe un PCA, ou il n'en existe pas. Dans le deuxième cas, l'audit est assez rapidement bouclé : l'audit émet des recommandations et fait en sorte que la direction s'intéresse au problème, et résolve ce dysfonctionnement.
Si un PCA existe, la question est : que couvre-t-il ? Est-il exhaustif ? Prend-il en compte les questions de redémarrage, les questions de *backup*, la gestion de crise et des scenarii de crise différents ?

Les problèmes ne se posent pas de la même façon en cas de pandémie ou d'inondation. Dans le deuxième cas une partie du personnel sera indisponible ; dans le premier, la totalité. D'ailleurs, dans le premier cas, c'est la totalité du système économique qui sera bloquée, et pas seulement le système bancaire. Bref, les scenarii varient, et leur probabilité aussi. L'analyse requiert une certaine compétence, notamment de la part des auditeurs.
L'autre point clé, au-delà des scenarii et des sujets qu'il va falloir analyser, c'est tout ce qui tourne autour de la communication de ce PCA.
Supposons qu'il en existe un. Comment a-t-il été diffusé dans l'entreprise ?
J'ai vu, dans des expériences plus ou moins récentes, de très bons PCA consignés dans plusieurs volumes, bien construits, argumentés, détaillés, mais pas diffusés (les volumes sont conservés dans un bureau fermé). Cela signifie que, en cas crise, la plupart des utilisateurs potentiels ou des gens concernés n'en auront pas connaissance, et ne sauront donc absolument pas quoi faire.
Procède-t-on à des tests de continuité ? Dans le monde où j'opère, oui. Ainsi, l'on fait des tests pour s'assurer que l'on peut contacter le directeur, des adjoints, les personnes qui savent faire redémarrer les systèmes, que tout le système fonctionne bien.
Autre point clé : la communication externe. Qui a le droit de parler, qu'a-t-on le droit de dire, à qui doit-on le dire ?
Je vais citer un exemple tout à fait dramatique, qui est le cas de l'incendie du tunnel du Mont-Blanc. La première communication qui a été faite à la presse disait : « Ce n'est pas grave, la situation est maîtrisée. » Il y avait quand même trente sept morts. Effectivement, cela aurait pu être pire, il aurait pu y avoir deux cents morts…Bref, la façon dont les faits on été relatés a été catastrophique.
Souvenez-vous maintenant de l'incendie du siège du Crédit lyonnais. La communication a été extrêmement bien maîtrisée sur le thème : « Nos activités redémarrent depuis Londres lundi matin. » On n'a pas entendu : « C'est épouvantable, c'est affreux… vous ne vous rendez pas compte, etc.», etc. C'est ce que j'appelle une bonne communication bien maîtrisée et c'est quelque chose qu'il faut prévoir et organiser.

Sur tous ces sujets, la Commission bancaire est de plus en plus attentive, parce qu'il y a des enjeux en termes de robustesse : c'est de la robustesse du système bancaire français qu'il s'agit. La compétitivité du système bancaire français, c'est important pour la Commission bancaire, comme c'est important pour tous les établissements bancaires.

Frédéric GEOFFROY

L'audit doit participer aux tests de continuité ; il a un rôle de monitoring. Dans certains pays, c'est une exigence réglementaire : l'audit doit faire un compte rendu sur le déroulement des tests et sur les observations qui ont été faites.
Il est particulièrement difficile d'organiser un test de continuité d'activité quand on est dans une configuration où les opérations sont traitées entre le centre, une succursale et une filiale, c'est-à-dire quand plusieurs implantations sont concernées.
Dans les plans de continuité d'activité, la partie informatique est bien définie, de même que la partie processus, l'implication des lignes métiers, des back-offices, de la comptabilité ; tout cela s'articule assez bien. En revanche, la validité, la pertinence des analyses d'impact sur le business, sur l'activité, sur la rentabilité, tous ces éléments sont très certainement perfectibles.
Enfin, si l'on revient au sujet précédent, l'externalisation, en matière de continuité d'activité, on constate que, chez les petits prestataires, les choses ne sont pas tout à fait organisées comme elles devraient l'être.

Claire VALTOT

Il est vrai que l'audit doit se préoccuper de l'existence d'un PCA chez les prestataires.
Une question subsidiaire et très intéressante est de savoir si leurs scenarii du PCA sont comparables aux nôtres ? Si nous envisageons trois scénarii de crises extrêmement graves comme l'inondation, la pandémie et la grève générale et que nos prestataires envisagent l'incendie et la panne de climatisation, et qu'il n'y a pas compatibilité, c'est comme s'ils n'avaient pas de PCA, pour nous. Il y a donc un problème de complémentarité et nous devons nous assurer de cette complémentarité-là.
Pour les prestataires, leur analyse du risque, c'est la qualité de la prestation et la continuité du service.
Notre enjeu à nous est différent : c'est la qualité du contrôle et l'existence de ce contrôle, quelles que soient les circonstances. Cette différence de *risk assessment*, qui est tout à fait normale compte tenu du fait que nous ne sommes pas dans le même univers, a des conséquences, notamment sur les PCA et leur compatibilité entre eux.

Patrice JOSNIN

Je reviens sur les tests transversaux. De fait, nous sommes de plus en plus interdépendants, et tester sur une place n'a plus beaucoup de sens. Dans un groupe, tester un PCA sur Paris implique de faire le même test à Londres et New York. Il faut absolument prendre en compte cette transversalité.
Je ne peux pas m'empêcher de boucler ce dernier thème avec le premier, car vous savez bien, tous, que les plans de continuité d'activité, leur robustesse, leur efficience, leur fiabilité ont évidemment un effet sur le capital alloué pour couvrir le risque opérationnel.

Question dans la salle

Pourrait-on avoir quelques informations complémentaires sur la rubrique : les hommes et la formation, s'il vous plaît ? Comment vous assurez-vous que les équipes sont correctement formées, en dehors de leur participation aux tests ?

Claire VALTOT

En dehors de la participation aux tests, j'observe qu'il y a un problème de diffusion du PCA : chacun sait-il ce qu'il doit faire dans tel ou tel cas ? Normalement, il est prévu dans le dispositif que les personnels soient identifiés selon leur fonction dans l'organisation et qu'ils reçoivent une information périodique ; chez moi, c'est au moins deux fois par an. Je reçois un document fort épais qui m'explique ce que je dois faire en cas de crise.
Les personnes qui font partie du plan de continuité d'activité sont individuellement prévenues et ont l'obligation de participer aux tests. Les tests tournent dans les différents départements, mais l'on ne mobilise pas toutes les ressources en faisant un test global qui serait trop onéreux. Les personnes et les fonctions sont référencées, leur niveau et ce qu'ils ont à faire est identifié, ainsi que le lieu où ils doivent se rendre. Les personnes sont également informées qu'elles doivent avoir deux exemplaires du document, un chez elles et un au bureau.
Effectivement il est difficile de s'assurer que les personnels ont reçu la bonne information au bon moment. Le système fonctionne un peu comme une cascade d'informations et de données à transmettre à ses équipes.

Patrice JOSNIN

Les échanges sur ces cinq thèmes nous amènent à un constat : les activités bancaires sont de plus en plus complexes à auditer, en raison notamment des risques systémiques diffus, donc difficiles à appréhender, à l'intérieur de nos établissements situés en France et à l'étranger.
C'est vrai à l'intérieur d'un établissement, c'est encore plus vrai à l'intérieur d'une communauté bancaire, et la communauté bancaire, on le sait bien, elle n'est plus nationale, mais mondiale.
C'est pourquoi les régulateurs incitent les équipes d'audit et d'inspection à être particulièrement vigilantes et attentives sur certaines zones de risques, dont les cinq zones que nous venons de passer en revue. Et les régulateurs nous demandent d'allouer, d'affecter les forces nécessaires. Il y a, sur ces points, une grande convergence des réglementations internationales.
Est-ce une contrainte ? Ou est-ce qu'au contraire cela ne renforce pas le rôle de la fonction audit inspection au sein de nos établissements, tant vis-à-vis de l'exécutif, de la direction générale, que de l'organe délibérant ?
Je crois que le rôle croissant des régulateurs ne vient pas contrecarrer notre plan d'action, qui découle toujours d'une approche par les risques. Simplement, les régulateurs balisent notre action, ils la jalonnent de thèmes clés, ils nous demandent de faire des focus sur des sujets qui leur paraissent essentiels parce qu'ils ont une vision très globale des risques systémiques et des dangers de contagion.
C'est certainement une marque de confiance de la part du régulateur de nous confier cette tâche et de s'appuyer sur nous. En réalité, le régulateur nous attribue de plus en plus de pouvoir dans l'entreprise. La tendance est plutôt de renforcer la position stratégique de l'audit, en en faisant un acteur de la gouvernance plutôt qu'en lui imposant des contraintes administratives.

Louis VAURS

Merci à Patrice, Claire, Frédéric et Michel pour la qualité de leur présentation. Je rejoins totalement, Patrice pour dire que les tâches supplémentaires que confie la commission bancaire à l'audit interne, accroissent ses pouvoirs dans l'entreprise mais aussi ses responsabilités.

Je vous informe pour terminer que la prochaine réunion avec la Commission bancaire se déroulera le 20 novembre 2007, dans l'après-midi.