

La fonction de conformité au sein des établissements de crédit et des entreprises d'investissement

INTRODUCTION : UN ENVIRONNEMENT QUI APPELLE LE RENFORCEMENT DE LA FONCTION DE CONFORMITÉ AU SEIN DU DISPOSITIF DE CONTRÔLE INTERNE

L'environnement dans lequel évoluent les banques les contraint à maîtriser un nombre croissant de techniques et de réglementations et à mettre en œuvre une politique de maîtrise des risques toujours plus rigoureuse. En effet, on observe au cours des dernières années :

- une diversification des métiers au sein des grands groupes du fait de rapprochements, de partenariats, d'acquisitions ;
- un enrichissement de l'offre de produits proposés aux différentes catégories de clients ;
- un développement des opérations complexes. Les opérations de financement structuré comme celles de titrisation pour compte de tiers faisant appel à des véhicules *ad hoc* se sont ainsi multipliées ; l'usage de nouveaux instruments sophistiqués s'est fortement développé au cours des dernières années ;
- une expansion géographique des implantations et des risques pris par les établissements ;
- une multiplication des agents économiques avec lesquels les établissements sont amenés à traiter, du fait par exemple de l'émergence au cours des dernières années de l'externalisation d'activités ;
- une intensification de la concurrence entre les établissements, ce qui se traduit par un renforcement des contraintes de rentabilité.

Au total, les établissements ont vu les risques qu'ils encourent s'accroître et se diversifier dans des cadres légaux en évolution. Cette tendance implique une très grande vigilance sur la conformité de leurs opérations.

Depuis quelques années, la plus grande fréquence des affaires imputables pour partie à un non-respect ou à une maîtrise insuffisante de la législation ou de la réglementation ainsi que les coûts externes financiers et de réputation de ces événements imposent aux entreprises industrielles et commerciales, mais aussi aux banques et aux régulateurs, de réfléchir aux modalités de maîtrise de ces risques.

Dans ce contexte, une réflexion a été engagée au niveau international, notamment au sein du Comité de Bâle, afin, d'une part, de mieux appréhender, dans le calcul des exigences de fonds propres, les risques autres que les risques de crédit et de marché et, d'autre part, de formuler des propositions spécifiques quant aux modalités de contrôle du risque de non-conformité. Le document consultatif du Comité de Bâle du 27 octobre 2003 sur la fonction de conformité dans les banques — *Consultative Document on the Compliance Function in Banks* — constitue une étape majeure de cette réflexion.

En France, le principe du respect de la conformité a été inscrit, dès 1997, dans le règlement n° 97-02 du Comité de la réglementation bancaire et financière relatif au contrôle interne. Les évolutions du cadre d'activité des banques appellent une réflexion, dans le contexte de celle conduite au niveau international, sur le contenu précis et les grands principes de mise en œuvre de la conformité. En particulier, du fait de l'importance et de la spécificité du risque de non-conformité aux lois et règlements, celui-ci paraît devoir être pris en charge par une fonction dédiée et, comme l'ensemble des risques encourus par les établissements de crédit et les entreprises d'investissement, être pleinement intégré dans le champ d'exercice du contrôle interne.

Le contrôle interne s'exerce, au moyen de la définition de procédures, de mesures et de limites de positions, sur :

- les risques de nature économique, tels que le risque de crédit ou les risques de marché ;
- les risques opérationnels, définis par le Comité de Bâle et repris dans la réglementation française (cf. l'étude du présent Rapport consacrée au risque opérationnel) ;
- les risques d'ordre juridique, dont font partie les risques de litige et le risque de non-conformité aux lois, règlements et normes professionnelles.

La présente étude est consacrée spécifiquement au risque de non-conformité. Elle examine les orientations possibles afin de mieux appréhender, mesurer et contrôler les risques de non-respect de lois ou de réglementations et de limiter leur impact. Elle revient tout d'abord, au regard des travaux conduits notamment au sein du Comité de Bâle et d'exemples de réglementations spécifiques élaborées récemment dans plusieurs pays, sur les modalités envisagées de réglementation du contrôle du risque de non-conformité. Elle rappelle ensuite le socle réglementaire français à partir duquel le contrôle du risque de non-conformité peut d'ores et déjà s'exercer. Elle essaie enfin, au vu de ces éléments et dans la perspective de la poursuite d'un renforcement du contrôle interne, de définir plusieurs pistes de réflexion quant aux modalités selon lesquelles le contrôle de ce type de risque pourrait s'organiser.

1. ÉTAT DES LIEUX EN MATIÈRE DE CONFORMITÉ

1.1. Le risque de non-conformité : un risque à définir

Le risque de non-conformité est défini par le Comité de Bâle¹ comme un risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, du fait de l'absence de respect des dispositions législatives et réglementaires, des normes et usages professionnels et déontologiques, propres aux activités des banques.

Le Comité de Bâle a réfléchi à la notion de risque de non-conformité.

Selon ce document, ceci inclut notamment les dispositions relatives à la prévention du blanchiment et au financement du terrorisme, la conduite des activités bancaires et financières (y compris les conflits d'intérêts), la protection de la vie privée et des données, voire, selon l'approche définie par l'établissement lui-même ou par le régulateur, la législation fiscale et le droit du travail.

Ainsi défini, le risque de non-conformité se distingue du risque juridique de litige avec une contrepartie puisqu'il ne vise pas la mise en cause des établissements au titre de leurs obligations contractuelles mais les conséquences dommageables du non-respect de règles relevant pour l'essentiel de l'ordre public.

La définition de la conformité utilisée dans le cadre de cette étude reprendra dans les grandes lignes celle du Comité de Bâle. La supervision bancaire s'intéresse naturellement plus spécifiquement au respect des dispositions spécifiques aux activités bancaires et financières.

1.2. Les établissements de crédit ont d'ores et déjà pris des dispositions pour réduire le risque de non-conformité

Les entreprises, notamment les banques, ont amélioré depuis plusieurs années leurs dispositifs de veille réglementaire afin d'approfondir la connaissance de la réglementation par leurs salariés et de formaliser davantage les procédures de contrôle de la conformité de leurs décisions à la réglementation ou aux lois. Comme le relève le Comité de Bâle, le risque de non-conformité fait désormais l'objet d'une gestion plus formalisée et identifiée de la part des établissements². Ce constat rejoint l'appréciation qui peut être portée sur la situation des banques françaises en la matière.

¹ Dans le document consultatif du Comité de Bâle du 27 octobre 2003 sur la fonction de conformité dans les banques « Consultative Document on the Compliance Function in Banks ».

² « Sound Practices for the Management and Supervision of Operational Risk » – « Saines pratiques de gestion et de contrôle du risque opérationnel » (février 2003) point 2.

Les établissements de crédit français ont commencé, sous l'impulsion notamment de la Commission bancaire, à mettre en œuvre des dispositifs de vérification de la conformité, ...

En effet, il ressort d'entretiens conduits avec les principaux établissements bancaires français que ceux-ci ont tous engagé, à des degrés divers, une réflexion quant aux modalités d'organisation d'un dispositif permettant de s'assurer de la conformité de leurs activités à la réglementation, à la loi, aux normes ou aux usages professionnels. La quasi-totalité des grands établissements se sont déjà dotés (ou sont en cours de désignation) d'un responsable de la conformité (le titre étant variable selon les établissements : responsable de la conformité ou « *compliance officer* », déontologue...). Les établissements de crédit français apparaissent cependant avoir des définitions hétérogènes de la conformité.

Chez un certain nombre d'entre eux, le champ d'intervention du responsable désigné de la conformité ou de la *compliance* se limite à la supervision du dispositif de prévention du blanchiment et à la déontologie, notamment dans l'acceptation du règlement général de l'ex-CMF¹. Le responsable dispose alors d'un nombre relativement limité de personnes pour l'assister.

... ils ont désigné des responsables internes, ...

Dans d'autres établissements, le responsable de la conformité est assisté d'équipes qui lui permettent d'avoir une vision (quasi) exhaustive des opérations du groupe. La définition du risque de non-conformité est élargie au contrôle de conformité des opérations aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques ainsi qu'aux orientations de l'organe délibérant ou de l'organe exécutif. Cela se traduit notamment par la consultation systématique, pour chaque opération nouvelle significative, d'un responsable du suivi du risque de non-conformité. Par ailleurs, les équipes présentes dans tous les métiers de l'établissement relaient le message du responsable de la conformité auprès des opérationnels. Plusieurs de ces établissements ont élaboré des procédures précisant les modalités du suivi de ce risque, voire une charte de la conformité.

... et certains ont mis en place un état de suivi adapté.

Enfin, quelques établissements, plus avancés encore, ont d'ores et déjà construit un état spécifique au suivi du risque de non-conformité. Ceci permet d'informer régulièrement les niveaux les plus élevés de l'établissement (organes exécutif et délibérant) du niveau de maîtrise de ce risque ainsi que de tout événement significatif relevant de cette problématique.

D'une manière générale, on observe une perception générale du risque de non conformité, même si les dispositifs mis en œuvre sont encore parfois insuffisamment réfléchis et a fortiori développés. Cette évolution s'explique essentiellement par les événements survenus au cours des dernières années, rappelés ci-dessus.

¹ CMF : Conseil des marchés financiers, désormais fusionné avec la COB (Commission des opérations de bourse) pour former l'AMF (Autorité des marchés financiers).

1.3. Un contexte international et réglementaire en évolution

Depuis plusieurs années, une meilleure prise en compte de la maîtrise de ce type de risque est au centre des réflexions internationales. À cet égard, le projet de Nouvel Accord sur les fonds propres (Bâle II) incite les établissements à améliorer les systèmes de mesure et de gestion des risques et à mieux appréhender l'ensemble des risques auxquels ils sont exposés. Ceci se traduit par la prise en compte dans les exigences de fonds propres non plus des seuls risques de crédit et de marché mais aussi des risques opérationnels.

Si l'on reprend la définition du risque opérationnel — risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs, y compris le risque juridique mais à l'exclusion des risques stratégiques et d'atteinte à la réputation — formulée dans le texte du troisième document consultatif du Comité de Bâle d'avril 2003, on peut considérer que le risque de non-conformité en relève, à tout le moins en partie.

Plusieurs groupes de travail internationaux ont, notamment dans la perspective de l'évolution du ratio de solvabilité, engagé une réflexion afin que les établissements aient une meilleure connaissance et une meilleure maîtrise de ce type de risques : d'abord plus spécifiquement pour les entreprises d'investissement (travaux conduits par le *CESR, Committee of European Securities Regulators*¹) et plus récemment pour les établissements de crédit au sein du Comité de Bâle.

1.3.1. Une réflexion a d'abord été plus particulièrement conduite pour les entreprises d'investissement

Le *CESR* s'est efforcé, dans une étude² parue en avril 2002, de définir les principales caractéristiques de la fonction *compliance*. Il ressort de ce document que cette fonction doit notamment :

- être indépendante des « opérationnels » ;
- informer les dirigeants de l'entreprise d'investissement ainsi que les contrôleurs internes et externes des résultats de ces contrôles ;
- adresser au régulateur un rapport sur les infractions significatives ;
- s'assurer régulièrement de l'adéquation des politiques et des procédures à la réglementation des services d'investissement.

Le CESR a défini les principales caractéristiques de la fonction compliance pour les entreprises d'investissement.

¹ Comité européen des régulateurs de valeurs mobilières.

² « *A European Regime of Investor Protection, The Harmonisation of Conduct of Business Rules* » (Un régime européen pour la protection de l'investisseur – L'harmonisation de l'application des règles de métier).

1.3.2. Le Comité de Bâle a récemment fait part de ses propositions en la matière

Le Comité de Bâle a formulé des principes relatifs à la fonction de conformité dans les banques.

Des réflexions sont également menées sur ce thème au sein du Comité de Bâle. En matière de risque opérationnel, il a publié un document de travail « *Sound Practices for the Management and Supervision of Operational Risk* » (février 2003). Par ailleurs, il a entrepris des travaux spécifiques sur la conformité.

En effet, un groupe de travail consacré à la fonction de conformité dans les banques a été constitué ; ce groupe, auquel des représentants du Secrétariat général de la Commission bancaire ont activement participé, a publié en octobre 2003 un document consultatif¹. Ce texte, qui a pour objet d'identifier les meilleures pratiques dans ce domaine et d'en favoriser la diffusion, énonce onze principes concernant la conformité.

- *L'organe délibérant doit superviser la gestion du risque de non-conformité. Il doit valider la stratégie de l'établissement. Il doit être informé au moins une fois par an de la politique de conformité et de ses modalités d'application.*
- *L'organe exécutif doit définir une ligne d'action en matière de « compliance » ; il doit s'assurer qu'elle est suivie et il doit en informer l'organe délibérant.*
- *L'organe exécutif doit organiser le contrôle du risque de non-conformité de manière permanente et efficace.*
- *Le statut de cette fonction doit être formalisé dans une charte ou un document approuvé par l'organe délibérant, définissant son positionnement, ses compétences et son rattachement hiérarchique.*
- *Elle doit être indépendante des équipes opérationnelles.*
- *Elle a pour objet d'identifier, d'évaluer et de suivre les risques de non-conformité encourus par l'établissement et de conseiller et de rendre compte à l'organe exécutif sur ce sujet.*
- *Le responsable de la fonction de conformité est en charge du suivi continu des activités liées à cette fonction. Le régulateur bancaire doit être informé de son départ.*
- *Le personnel mis à sa disposition doit avoir les compétences, l'expérience et les qualités professionnelles et personnelles permettant d'assumer cette fonction.*
- *Ce dispositif doit permettre aux établissements ayant une activité internationale de gérer de manière satisfaisante le risque de non-conformité en se conformant aux règles locales.*
- *L'activité de la fonction de conformité doit être incluse dans le champ du contrôle interne.*
- *Certaines activités de la fonction de conformité peuvent éventuellement faire l'objet d'une externalisation. Le responsable de la fonction de conformité doit être salarié de l'établissement.*

¹ « *Consultative Document on the Compliance Function in Banks* », 27 October 2003.

L'objectif du Comité de Bâle, en publiant pour consultation un tel document, est de favoriser la diffusion, au sein des établissements de crédit, d'une « culture de conformité » afin qu'elle se traduise, formellement, par une attention accrue portée à ce risque. L'intention du Comité de Bâle est de veiller à ce que cette fonction soit bien assurée. L'attention des établissements est attirée sur le fait qu'il s'agit — par nature — d'une fonction indépendante des activités opérationnelles, dont le rattachement hiérarchique doit être très élevé, mais dont le fonctionnement est inclus dans le champ d'investigation de l'audit/inspection interne.

1.4. Des réglementations spécifiques au risque de non-conformité existent déjà

Il ressort d'une étude conduite par Price Waterhouse Coopers¹ sur la réglementation en matière de conformité dans une douzaine de pays occidentaux que, dans la moitié de ceux-ci, une réglementation spécifique a été élaborée.

Selon cette étude, les États-Unis ont commencé, dès les années 1930-1940, à élaborer une réglementation en matière de *compliance* enrichie au fil des ans. Plus près de nous et au cours des dernières années, plusieurs pays, notamment le Royaume-Uni et la Belgique, ont développé un cadre réglementaire autour de la fonction de conformité.

1.4.1. La réglementation en matière de conformité au Royaume-Uni

Au Royaume-Uni, la réglementation² définit les obligations des établissements en matière de conformité : une entreprise doit établir et maintenir un dispositif de contrôle de la conformité de ses opérations avec les textes prévus par la réglementation afin de prévenir tout risque que l'entreprise soit utilisée à des fins criminelles³.

La nature du dispositif de mesure et de contrôle des risques mis en œuvre dépend de la nature, du volume et de la complexité de l'activité, de la diversité (y compris géographique) des opérations et du degré de risque associé à chaque métier. Ces dispositions se traduisent pour la très grande majorité des entreprises du secteur financier britannique par la nomination d'un *compliance officer* (responsable de la conformité).

Au Royaume-Uni, l'ampleur du dispositif dépend du volume et de la nature des opérations réalisées.

Si la nature, le volume ou la complexité de l'activité l'exigent, la création d'un département propre, en charge du risque de non-conformité, est demandée. Il doit être suffisamment indépendant pour remplir sa mission efficacement. Il convient de formaliser ses modalités d'organisation et d'activité. Il doit disposer de moyens suffisants. Il doit avoir accès à toute l'information qui lui est nécessaire.

¹ « *Regulatory Compliance: Adding value* » (Conformité réglementaire : faire mieux).

² Chapitre 3 « *Systems and controls* » de la réglementation du *Financial Services Authority (FSA)*.

³ « *A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.* »

Son responsable, dont la nomination est approuvée par le FSA, a accès direct au Conseil d'administration.

Son responsable, dont la nomination est approuvée par le *Financial Supervisory Authority (FSA)*¹, doit avoir un accès direct au conseil d'administration. La responsabilité de la fonction doit être exercée par un cadre dirigeant et elle ne peut pas être externalisée.

Ce responsable participe à l'élaboration de solutions aux problèmes réglementaires rencontrés par l'établissement. Il a pour mission de fournir des conseils aux différents départements de l'établissement en matière de respect de la réglementation. Il aide la société à conduire ses activités en conformité avec les lois, règlements et codes de déontologie. Il est enfin un des interlocuteurs du régulateur dans l'établissement.

1.4.2. La réglementation en matière de conformité en Belgique

En Belgique, la compliance est en charge de l'examen et de l'amélioration du respect des règles relatives à l'intégrité du métier de banquier.

En Belgique, la Commission bancaire et financière a rendu publique en décembre 2001 une circulaire² définissant les principes auxquels la fonction de *compliance* des établissements de crédit doit répondre. Les principaux points de cette réglementation sont les suivants.

- La *compliance* est une fonction indépendante au sein de l'organisation, axée sur l'examen et l'amélioration du respect par l'établissement des règles relatives à l'intégrité du métier de banquier.
- Dans le cadre de sa mission de surveillance, le conseil d'administration vérifie régulièrement si l'établissement dispose d'une fonction de *compliance* adéquate. Le comité de direction prend les mesures nécessaires à cette fin.
- Le comité de direction élabore une politique d'intégrité dans une note de politique qui est régulièrement actualisée.
- Il informe le conseil d'administration au moins une fois par an de l'état de la situation en matière de *compliance*, le cas échéant par l'intermédiaire du comité d'audit.
- Le département *compliance* doit disposer, au sein de l'organisation, d'un statut adapté, garanti par un document approuvé par le comité de direction et confirmé par le conseil d'administration.

Le Comité de direction est très impliqué dans cette fonction...

... qui est assurée par une cellule permanente spécialement dédiée.

Au total, il ressort que plusieurs pays ont d'ores et déjà élaboré des réglementations spécifiques en matière de contrôle de conformité, qui présentent plusieurs points communs. En particulier, le périmètre des activités de la structure en charge du contrôle de conformité doit être clairement défini, cette structure doit être indépendante et organisée de manière adaptée à l'entreprise. Son rattachement hiérarchique doit être très élevé et elle doit être distincte de l'audit interne.

¹ Autorité de supervision financière, en charge de la supervision des secteurs bancaire et des assurances ainsi que des marchés de capitaux au Royaume-Uni.

² Circulaire D1 2001/13.

2. LA FRANCE DISPOSE D'ORES ET DÉJÀ D'UN SOCLE RÉGLEMENTAIRE POUR ENCADRER LES MODALITÉS DE CONTRÔLE DU RISQUE DE NON-CONFORMITÉ

La réglementation française a précisé les exigences minimales en matière de contrôle interne au cours des dernières années et a incité les banques à mettre en place des dispositifs de maîtrise des risques adaptés aux risques encourus. Plusieurs références réglementaires peuvent à cet égard servir de base à la construction d'un dispositif de maîtrise du risque de non-conformité : le règlement n° 97-02 du Comité de la réglementation bancaire et financière (CRBF) relatif au contrôle interne, le titre III du règlement de l'ex-Conseil des marchés financiers (CMF), la réglementation relative à la prévention du blanchiment et, plus récemment, la loi de sécurité financière.

2.1. Les exigences en matière de contrôle interne ont été précisées en France avec le règlement n° 97-02, étendu aux entreprises d'investissement en 2001 (règlement n° 2001-01)

L'entrée en vigueur du règlement n° 97-02 a constitué une étape majeure du renforcement de la surveillance des risques et de l'efficacité des contrôles au sein des établissements de crédit et des entreprises d'investissement.

En effet, ce texte prévoit tout d'abord l'obligation pour les établissements de se doter d'un dispositif de contrôle interne (ses caractéristiques sont détaillées dans les titres II à VI du règlement), dont ils doivent s'assurer du caractère adapté à leur activité, leurs risques, leur taille.

Conformément aux articles 7 à 11 du règlement n° 97-02, les unités en charge du contrôle interne doivent être indépendantes, disposer de moyens adaptés leur permettant d'assurer un contrôle exhaustif des risques et d'examiner périodiquement les systèmes de contrôle mis en place. De par la définition même de leur fonction, elles doivent participer à la maîtrise de tous les risques encourus par l'établissement, y compris ceux de non-conformité.

L'article 5 du règlement prévoit spécifiquement dans les missions du dispositif de contrôle interne que celui-ci doit :

« Vérifier que les opérations réalisées par l'entreprise, ainsi que l'organisation et les procédures internes sont conformes aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques et aux orientations de l'organe délibérant ou de l'organe exécutif. »

Le règlement n° 97-02 intègre déjà l'obligation d'un dispositif de contrôle du risque de non-conformité.

Le règlement n° 97-02 prévoit par conséquent explicitement le contrôle du risque de non-conformité par les établissements.

Enfin, ainsi que prévu par les articles 38 et 39 du règlement précité, l'organe délibérant doit procéder à l'examen des informations transmises par l'organe exécutif en matière de contrôle interne. Dans ce cadre, l'organe délibérant doit donc être informé des mesures adoptées en matière de conformité.

La loi de sécurité financière — avec l'obligation pour le président de l'organe délibérant de rédiger un rapport dans lequel il rend compte des conditions de préparation et d'organisation des travaux de l'organe délibérant ainsi que des procédures de contrôle interne mises en place par la société — est dans la continuité des exigences introduites par le règlement n° 97-02 en matière de contrôle interne. On doit considérer, là encore, que les informations relatives à la maîtrise du risque de non-conformité devraient figurer dans ce document.

2.2. Le règlement général de l'ex-CMF précise les attentes en matière de déontologie

Les règles déontologiques des prestataires de services d'investissement ont été définies.

Avec le titre III du règlement de l'ex-CMF, relatif aux règles de bonne conduite à suivre, les obligations des prestataires de services d'investissement en matière de déontologie ont été définies. Ceux-ci doivent désigner un responsable de la déontologie. Ses missions sont notamment définies par l'article 3-1-3 :

- identification des dispositions d'ordre déontologique nécessaires au respect des règles de bonne conduite ;
- établissement d'un recueil de l'ensemble des dispositions déontologiques que doivent observer le prestataire habilité, les personnes agissant pour son compte ou sous son autorité et ses mandataires [...] agissant dans le cadre du service d'investissement ;
- diffusion de tout ou partie de ces dispositions auprès des collaborateurs et des mandataires du prestataire habilité ;
- contrôle du respect par le prestataire habilité, ses collaborateurs et ses mandataires de l'ensemble des règles de bonne conduite et de la mise en œuvre des dispositions appropriées en cas de manquement à ces règles ;
- réalisation, indépendamment des missions de contrôle, de missions d'assistance et d'orientation ayant pour objet de guider les collaborateurs du prestataire habilité pour l'application des règles de bonne conduite.

2.3. Les exigences en matière de prévention du blanchiment sont très précises

Au cours des dernières années, les exigences en matière de prévention du blanchiment ont été précisées. Elles concernent notamment :

- l'identification et la connaissance de la clientèle ;
- l'examen des opérations atypiques ;
- l'obligation de déclaration des opérations suspectes à Tracfin ;
- la constitution de dossiers de renseignements ;
- l'obligation de se doter d'une organisation et de procédures internes en la matière ;

- la conservation des documents et justificatifs pendant au moins cinq ans ;
- la désignation d'un ou plusieurs correspondants Tracfin.

Ces obligations ont été renforcées récemment par le règlement n° 2002-01 du Comité de la réglementation bancaire et financière — CRBF — relatif au contrôle des chèques, par le règlement n° 2002-13 relatif à la monnaie électronique et par la loi du 11 février 2004 sur l'identification en matière de banque à distance. Le respect de l'ensemble de ces obligations par les établissements les a conduits à renforcer les dispositifs de prévention du blanchiment.

Les obligations en matière de prévention du blanchiment ont été récemment encore renforcées.

Par ailleurs, il convient de noter que des renforcements réglementaires sont envisagés en matière de banque à distance et de transparence des transferts de fonds. Par ailleurs, la transposition des recommandations du Comité de Bâle sur la connaissance de la clientèle et des quarante recommandations révisées du Gafi ¹ devrait être effectuée prochainement.

La France dispose donc d'ores et déjà de plusieurs textes qui prévoient — le plus souvent implicitement — le contrôle de la conformité des transactions des établissements à la réglementation. Toutefois, ces textes ne définissent pas encore précisément les obligations spécifiques des établissements en matière de maîtrise et de contrôle du risque de conformité et le champ de celui-ci.

2.4. Dans le cadre de l'instruction des demandes d'agrément et de changement de contrôle, le Comité des établissements de crédit et des entreprises d'investissement (CECEI) prête également attention à l'existence d'un dispositif de vérification de la conformité adapté à la taille et aux activités des demandeurs

Le CECEI prête attention à ce que la présentation de l'organisation interne des demandeurs comprenne une description des fonctions de contrôle interne, qui peuvent inclure celle de conformité aux côtés de celle d'audit/inspection ou des autres types de contrôles internes permanents, surtout lorsque la taille ou la multiplicité des activités accroissent l'importance potentielle des risques de cette nature.

¹ Gafi : Groupe d'action financière sur le blanchiment des capitaux.

3. IL EXISTE DIFFÉRENTES PISTES POSSIBLES POUR RENFORCER LES MOYENS MIS EN ŒUVRE POUR LIMITER LE RISQUE DE NON-CONFORMITÉ

Les moyens mis en œuvre pour limiter le risque de non-conformité relèvent de la responsabilité des dirigeants.

Il n'appartient pas à la Commission bancaire de déterminer les choix de gestion des établissements, ni de définir les procédures internes de ceux-ci ; cette responsabilité incombe aux organes sociaux. En revanche, la Commission bancaire attache depuis de longues années une attention toute particulière à la qualité du dispositif de contrôle interne, et notamment à sa capacité de « vérifier que les opérations réalisées par l'entreprise, ainsi que l'organisation et les procédures internes sont conformes aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques et aux orientations de l'organe exécutif » (article 5a du règlement n° 97-02 relatif au contrôle interne).

Il paraît indispensable, d'une part, de tirer des enseignements de l'évolution de l'environnement français et international en matière d'exigence de conformité, d'autre part, de prendre en compte l'état d'avancement des réflexions en la matière.

À partir des travaux engagés par le Comité de Bâle et de la pratique de nombreux établissements en la matière, et compte tenu des discussions constructives engagées avec nombre de groupes bancaires au cours des derniers mois, il est possible de définir des pistes de réflexion sur les caractéristiques que pourrait présenter une fonction en charge de la mesure, de la maîtrise et du contrôle du risque de non-conformité.

3.1. La supervision bancaire contribue fortement à la mise en œuvre d'une fonction interne de contrôle de la conformité

Au terme de l'examen rapide de l'état des lieux en matière de conformité, le risque de non-conformité peut être défini comme un risque de non respect des dispositions réglementaires applicables aux activités bancaires et financières, y compris celles relatives à la prévention du blanchiment et du financement du terrorisme, des normes et usages professionnels et déontologiques.

La supervision bancaire doit à tout le moins s'attacher à la vérification du principe de conformité pour tout ce qui relève spécifiquement de l'activité bancaire et financière, dans le cadre du dispositif plus général du contrôle interne permanent des opérations.

Par ailleurs, ainsi que le rappelle le Comité de Bâle, il convient, concomitamment à la mise en place d'une fonction de conformité (et conformément à l'article 40 du règlement n° 97-02), d'en définir les attributions de manière formalisée. Cette formalisation peut, par exemple, prendre la forme d'une charte dont tous les membres du personnel devront être destinataires.

3.1.1. Un champ d'exercice de la fonction couvrant tous les secteurs, toutes les zones géographiques et tous les contextes réglementaires du groupe

Le champ d'exercice de la fonction de conformité doit être exhaustif. Il doit intégrer non seulement les métiers de banque de financement et d'investissement, pour lesquels les établissements ont souvent déjà mis en œuvre des dispositifs, mais aussi les autres activités. Il est ainsi nécessaire — et l'actualité récente a encore mis l'accent sur ce point — de porter une grande attention aux risques de conflits d'intérêts dans le cadre de l'activité de banque d'affaires. L'exercice d'une activité de banque de détail implique une connaissance des législations afférentes, par exemple le droit de la consommation. D'une manière générale, il convient de veiller à la prévention des risques éventuels de conflits d'intérêts entre les différents métiers et implantations de la banque.

Le champ d'application de l'activité couvre tous les secteurs, toutes les zones géographiques et tous les contextes réglementaires du groupe.

Pour tous ces métiers, le champ d'investigation doit être mondial. Les entreprises assujetties s'assurent que leurs filiales et succursales à l'étranger mettent en place des dispositifs de contrôle de la conformité de leurs opérations qui respectent les dispositions locales applicables à leur activité. En outre, il convient, en cas d'opération de croissance externe, que l'entité acquise soit intégrée le plus rapidement possible au dispositif de contrôle interne, y compris en ce qui concerne le risque de non-conformité.

Le champ d'action de la fonction de conformité doit être mondial et n'exclure aucun métier.

Si l'externalisation d'activités peut permettre de réduire certains risques, en profitant de l'expertise de spécialistes, les opérations effectuées par le sous-traitant restent sous la responsabilité de la banque. L'externalisation d'une activité auprès d'un partenaire ne respectant pas la réglementation peut l'exposer à un risque de réputation non négligeable. Ce risque peut être d'autant plus important que le partenaire sera dans un pays étranger, dont l'établissement n'aura pas forcément la maîtrise de la réglementation. L'établissement doit par conséquent prendre en compte ces « démembrements » dans sa politique de maîtrise du risque de conformité et plus largement de contrôle interne.

3.1.2. Une contribution générale au renforcement d'une culture de la conformité

Outre la supervision du dispositif de prévention du blanchiment et les missions relatives à la déontologie, l'une des principales fonctions de la fonction *compliance* doit être la contribution à l'émergence ou au renforcement d'une culture de la conformité au sein de l'établissement.

À cette fin, une sensibilisation de tout le personnel au travers d'actions de formation et une actualisation régulière des connaissances des agents au fur et à mesure des évolutions réglementaires doivent être organisés.

Il convient en outre d'être attentif au fur et à mesure du développement de nouvelles activités et de l'apparition de nouvelles implantations — notamment dans des pays desquels l'établissement était jusque-là absent — que le personnel dispose effectivement de toute la connaissance réglementaire et législative nécessaire à l'exercice de ces nouvelles activités et qu'à défaut la formation appropriée soit mise en œuvre le plus rapidement possible. Il convient également que les dirigeants des entreprises puissent s'assurer de l'actualisation régulière des connaissances de leurs collaborateurs en la matière. Une attention toute particulière

Une attention particulière doit être portée aux activités et implantations nouvelles.

doit en outre être portée aux opérations transfrontières, qui exigent le respect de plusieurs réglementations ou législations.

Enfin, une charte ou un recueil de procédures doivent être établis et largement diffusés.

3.1.3. Une activité de conseil et de contrôle ex ante

La fonction de conformité doit avoir un rôle de conseil.

Avant qu'un établissement développe un nouveau produit ou modifie profondément un produit existant, qu'il noue une relation commerciale avec un nouveau client ou une nouvelle catégorie de contreparties, qu'il décide d'externaliser une activité, il est souhaitable que l'établissement de crédit ou l'entreprise d'investissement s'assure que cette opération ne le met pas en infraction à une loi ou à un règlement, ne l'expose pas à un risque de réputation, ne se traduit pas par un conflit d'intérêts. L'une des missions du responsable central, ou le cas échéant local ou spécialisé pour le métier considéré, de la vérification de la conformité, paraît devoir être de procéder à ce type d'examen *ex ante* de façon à conseiller les échelons hiérarchiques considérés, y compris l'organe exécutif.

Il serait ainsi souhaitable que se généralise la pratique consistant pour les établissements à prévoir des procédures spécifiques d'examen de la conformité, notamment d'approbation préalable systématique, pour les produits nouveaux ou fortement modifiés. Ainsi que de nombreux établissements le font déjà, il paraîtrait utile de systématiser la pratique des comités « nouveau produit », auxquels un représentant de la fonction de conformité doit participer.

3.1.4. La mise en œuvre d'une information interne adaptée

Le suivi du risque de conformité par l'organe exécutif ne constitue qu'une de ses nombreuses responsabilités. Il doit disposer d'une information fiable et synthétique afin de hiérarchiser rapidement les risques et de s'assurer que la politique de conformité mise en œuvre au sein de son établissement permet de détecter les éventuelles anomalies et surtout de les prévenir.

Les établissements doivent tout d'abord identifier parmi leurs opérations les zones de risques ainsi que leur degré de vulnérabilité. Il convient par conséquent que la fonction de conformité participe à l'élaboration d'une cartographie des risques de non-conformité.

L'organe exécutif et l'organe délibérant doivent disposer d'une information spécifique sur le suivi du risque de non-conformité.

Il importe par ailleurs que les établissements se dotent d'outils d'information spécifiquement conçus pour le suivi du risque de non-conformité. Il est également nécessaire que l'organe exécutif soit rapidement informé de la découverte d'éventuelles infractions et qu'une déclaration rapide des incidents concernant le respect des lois françaises ou étrangères soit faite, lorsque la loi ou la réglementation l'exige, aux autorités compétentes.

Les établissements doivent s'attacher à élaborer un suivi des opérations les plus porteuses de risques de non-conformité : opérations complexes, par exemple, opérations d'investissement et de désinvestissement financier, opérations transfrontières... Il convient également de mettre en place un suivi des mesures correctives mises en œuvre à la suite de la détection de défaillances. Ce système, pour être pleinement efficace, doit être mondial.

3.2. Une indépendance à assurer

La fonction en charge de la maîtrise et du contrôle du risque de non-conformité doit être indépendante des services opérationnels, ainsi que précisé dans les réglementations rappelées dans cette étude et dans les documents de travail du CESR et du Comité de Bâle.

À l'image de ce qui est prévu pour le contrôle interne (article 7 du règlement n° 97-02), le rattachement hiérarchique du responsable central de la conformité doit être le plus élevé possible, afin d'en garantir l'indépendance. Il semble souhaitable, ainsi que le suggère le document consultatif du Comité de Bâle, que la responsabilité au plus niveau de la conformité soit assurée par un membre de l'organe exécutif.

Il convient également d'assurer dans les groupes l'indépendance des *compliance officers* présents dans les unités opérationnelles. Pour cela, il pourrait être envisagé que leur rémunération et le déroulement de leur carrière soient décidés soit par les responsables de la conformité groupe soit, à tout le moins, avec leur avis conforme.

Que le responsable de cette fonction soit ou non membre du comité exécutif, il convient qu'il ait un accès privilégié à l'organe exécutif de l'établissement, afin de l'informer des éventuelles défaillances.

Si l'indépendance est une condition indispensable au bon fonctionnement d'une fonction de conformité, il importe également que celle-ci soit facilement accessible pour tous les collaborateurs de l'établissement. Il paraît envisageable à cet égard de protéger les agents qui souhaitent informer un responsable du contrôle de la conformité d'une éventuelle défaillance du dispositif ou d'une malversation (cf. protection des « *whistle blowers* » dans la loi Sarbarnes Oxley).

Le positionnement hiérarchique du responsable de la conformité doit en garantir l'indépendance, ...

... lui assurer un accès direct à l'organe exécutif...

... et une disponibilité à l'égard de l'ensemble des collaborateurs.

3.3. Une fonction qui devra être adaptée à la nature de chaque établissement

Les propositions de création d'une fonction « compliance » formulées dans le document du Comité de Bâle ont pu être perçues comme plus particulièrement adaptées aux grands établissements internationaux. La problématique de la conformité des décisions des établissements de taille plus modeste n'en reste pas moins pertinente. Elle est même parfois encore plus prégnante du fait, d'une part, de la plus grande difficulté pour les établissements de taille modeste à mettre en œuvre une séparation des fonctions effectives et, d'autre part, à disposer de toutes les compétences pour parfaitement maîtriser la réglementation et ses évolutions. Il convient par conséquent de réfléchir également dans ce cas aux modalités d'adaptation d'un système de maîtrise du risque de non-conformité.

Le dispositif de suivi du risque de non-conformité s'inscrivant largement dans le cadre du dispositif de contrôle interne permanent, il paraît envisageable d'appliquer des dispositions similaires à celles prévues par l'article 8 du règlement n° 97-02 pour le dispositif de contrôle interne, dans le cas d'établissements de taille modeste ou appartenant à des groupes.

Le risque de non-conformité concerne tous les établissements, y compris les plus petits, sous une forme adaptée à chacun.

L'organisation de la fonction de conformité doit être cohérente avec l'organisation générale de l'établissement et, le cas échéant, de son groupe d'appartenance.

Lorsque la taille de l'entreprise ne justifie pas de confier cette responsabilité à une personne spécialement désignée, le responsable du contrôle interne permanent semble devoir assurer la coordination de tous les dispositifs qui concourent à l'exercice de la fonction de contrôle de la conformité.

Lorsqu'une entreprise appartient à un groupe au sens de l'article 1^{er} du règlement n° 2000-03 ou relève d'un organe central, cette responsabilité pourrait être assurée au niveau d'une autre entreprise du même groupe ou affiliée au même organe central, après accord des organes délibérants des deux entreprises concernées.

Les modalités d'organisation peuvent varier d'un établissement à un autre : certains ont adopté une structure fortement décentralisée ; d'autres, au contraire, ont mis en place une équipe centrale développée. Cette organisation, quelle qu'elle soit, devra garantir l'indépendance des agents en charge du contrôle de la conformité. Il paraît néanmoins nécessaire, pour que celle-ci soit aussi forte dans tous les métiers et implantations d'un groupe bancaire et que ses méthodes soient homogènes, qu'une coordination soit assurée.

3.4. Une implication des plus hautes instances de l'établissement

De même que pour le contrôle interne, il appartient aux organes exécutif et délibérant de veiller à la mise en place de systèmes efficaces de maîtrise et de contrôle des risques. Cette implication de l'organe délibérant et de l'organe exécutif et le soutien qu'ils peuvent apporter à la fonction de conformité conditionnent très largement l'efficacité de celle-ci.

L'organe délibérant doit être tenu informé du suivi du risque de non-conformité par l'organe exécutif...

L'organe délibérant doit tout d'abord disposer d'une information suffisante, complète et synthétique quant au suivi et aux contrôles du risque de non-conformité. Conformément à l'article 38 du règlement n° 97-02, l'organe délibérant doit procéder à l'examen de l'activité et des résultats du contrôle interne — et donc entre autres du contrôle de la conformité — sur la base des informations qui lui sont transmises par l'organe exécutif et par les responsables du contrôle interne et de la conformité. De même, conformément à l'article 39 du règlement n° 97-02, « l'organe exécutif d'un établissement doit informer, au moins une fois par an, l'organe délibérant, et le cas échéant le comité d'audit, des éléments essentiels et des enseignements principaux qui peuvent être dégagés des mesures de risques auxquels l'entreprise, et le cas échéant le groupe, sont exposés. ». Il convient, là encore, que les éléments relatifs au risque de non-conformité figurent dans cet état de suivi. L'examen des informations relatives au risque de non-conformité peut être délégué au comité d'audit ou à un comité, spécifique à la conformité, émanation de l'organe délibérant.

... qui définit les modalités d'application de la politique de conformité et en vérifie l'efficacité.

Il convient que l'organe exécutif définisse les modalités d'application de la politique de conformité et qu'il s'assure, à tout le moins une fois par an, que le dispositif de contrôle interne examine régulièrement le dispositif de conformité. Cette implication est indispensable au succès de la diffusion d'une culture de la conformité au sein de l'entreprise.

3.5. La fonction de conformité doit disposer de moyens suffisants

Il importe que les moyens affectés à la fonction de contrôle du risque de non-conformité par les établissements leur permettent d'assurer une couverture suffisante de ce risque au sein de toutes les entités. Afin d'assurer la crédibilité des agents en charge de la conformité, ceux-ci doivent être parfaitement capables de maîtriser les opérations qui sont soumises à leur examen. À cet égard, la présence d'anciens opérationnels parmi les équipes et plus largement la diversité des profils des agents constituent des atouts.

La formation et l'expérience des agents mis au service de la fonction de conformité sont déterminants pour la crédibilité de celle-ci.

On peut noter que les établissements de crédit s'efforcent de rassembler au sein des équipes en charge de la conformité des personnels dont les profils sont complémentaires : agents ayant une formation de juristes, anciens auditeurs internes ou externes, anciens opérationnels.

D'importants progrès restent toutefois à accomplir en matière d'allocations de moyens suffisants à la fonction de conformité afin que la prise en compte de toutes les implantations et de tous les métiers soit assurée dans des conditions pleinement satisfaisantes.

3.6. Une fonction « auditable »

L'audit ou inspection interne des établissements a un rôle essentiel à jouer dans le dispositif de maîtrise du risque de non-conformité. Il doit en particulier vérifier le bon fonctionnement du dispositif de contrôle interne.

Conformément à l'article 11 du règlement n° 97-02, il convient que les entreprises assujetties procèdent à un réexamen régulier des systèmes de mesure des risques et de détermination des limites, y compris pour les risques de non-conformité, afin d'en vérifier la pertinence au regard de l'évolution de l'activité, de l'environnement des marchés ou des techniques d'analyse. Les organes exécutif et délibérant doivent en outre disposer des éléments leur permettant d'apprécier la pertinence de la méthodologie de mesure des risques et du dispositif de contrôle de la conformité.

Il paraît par conséquent indispensable que la fonction de conformité soit « auditable », à l'instar des autres activités d'un établissement. Si l'on veut que l'audit (ou inspection) puisse juger en toute indépendance de l'efficacité du dispositif de conformité — il devra notamment s'assurer que le responsable de la conformité participe efficacement à la diffusion d'une culture de la conformité — et de la pertinence des moyens qui lui sont alloués, il apparaît souhaitable (à l'exception des entreprises de taille la plus modeste et n'appartenant pas un groupe) que les responsables de l'audit et de la conformité soient distincts.

La fonction de conformité s'inscrit dans le champ d'investigation de l'audit interne.

CONCLUSION

La réflexion en matière de contrôle du risque de non-conformité, aussi bien du côté des régulateurs bancaires aux niveaux international (Comité de Bâle) et national que des établissements eux-mêmes, est déjà largement engagée. Elle peut s'appuyer, à tout le moins en France, sur un principe réglementaire établi à l'article 5 du règlement n° 97-02 du Comité de la réglementation bancaire et financière et sur la sensibilisation et l'expérience des établissements de crédit et des entreprises d'investissement français.

Du fait de l'évolution de l'activité des établissements, dans la perspective d'un renforcement des efforts engagés et d'un alignement sur les meilleurs standards internationaux, plusieurs éléments paraissent d'ores et déjà pouvoir être soulignés :

- si la fonction de contrôle de conformité doit être indépendante et couvrir de manière exhaustive le risque de non-conformité au sein d'un établissement, il n'existe pas de schéma unique d'organisation car celle-ci doit avant tout prendre en compte les activités et la taille des entreprises ;
- la fonction de conformité doit jouer un rôle croissant au sein des établissements assujettis, lors du choix des nouvelles opérations comme au cours de la vie de l'entreprise, au niveau national comme international ; elle doit faire l'objet de procédures de formation, d'information, d'édiction de normes internes et de contrôle permanent ;
- l'implication des organes exécutif et délibérant est indispensable ;
- la conformité doit être un élément fort de la culture de l'entreprise, ce qui signifie que les efforts doivent être constamment renouvelés en la matière.

De la même façon que les investissements consentis en matière de maîtrise des risques de crédit et de marché au cours des dernières années ont permis aux établissements de mieux les sélectionner et les mesurer, les efforts qui doivent être poursuivis en matière de contrôle de la conformité permettront aux établissements de maîtriser ce risque croissant à l'échelle mondiale mieux encore qu'aujourd'hui, et participeront ainsi au maintien de la très haute qualité de la place bancaire et financière française.

Ces efforts doivent être rapprochés des développements réalisés dans la perspective de la préparation au nouveau ratio de solvabilité, notamment en ce qui concerne les risques opérationnels.

Enfin, ils doivent s'inscrire dans le cadre, plus général, des actions engagées dans tous les secteurs économiques en matière d'amélioration des pratiques de gouvernance d'entreprise.