# Contrôle interne : nouvelles avancées dans le secteur bancaire et financier

Gilles VAYSSET*

Les établissements de crédit et les entreprises d'investissement (définis pour les besoins du présent article comme les « établissements financiers ») sont invités cette année à accomplir un saut qualitatif majeur en matière de contrôle interne, 8 ans après les premières prescriptions formulées dans ce domaine par le règlement du 21 février 1997 n° 97-02 du Comité de la réglementation bancaire et financière (CRBF), qui leur est applicable depuis le 1er octobre 1997. C'est, en effet, au 1er janvier 2006 qu'est entré en vigueur l'arrêté du ministre de l'Économie, des Finances et de l'Industrie du 30 mars 2005, portant modification du règlement n° 97-02 : cet arrêté vient compléter et préciser le règlement relatif au contrôle interne des établissements de crédit et des entreprises d'investissement. Bien au-delà d'une actualisation, cette réforme témoigne de la percée de nouvelles préoccupations des autorités de supervision. Il s'agit d'ailleurs d'un des tout premiers textes réglementaires d'importance pour la profession bancaire et financière sur lequel le nouveau Comité consultatif de la législation et de la réglementation financières (CCLRF) a eu à donner son avis, le 25 février 2005, conformément au nouveau dispositif institutionnel mis en place en application de la loi de sécurité financière[1].

Quelles sont les grandes nouveautés que cet arrêté apporte en ce domaine ? Les obligations additionnelles couvrent les trois domaines suivants : risque de non conformité, risque d'externalisation, articulation des contrôles permanent et périodique.

* Secrétaire général du Comité consultatif de la législation et de la réglementation financières (CCLRF). L'auteur n'engage pas le Comité.

## LES TROIS DOMAINES DES NOUVELLES OBLIGATIONS

### Le risque de non conformité

Le nouveau règlement n° 97-02 formalise et renforce la nécessité d'outils performants de maîtrise du risque de non conformité. La réforme du contrôle de ce risque s'imposait en raison des évolutions récentes des pratiques des acteurs financiers et des attentes du public. Comme on l'a vu ces dernières années, le secteur financier a été confronté à la fois à une recrudescence d'affaires liées au non respect des réglementations applicables et à un coût croissant de leurs suites, amiables ou contentieuses (c'est en milliards de dollars que s'établit, pour certaines banques nord-américaines, le coût des affaires Enron ou WorldCom), sans parler des contraintes que cela peut faire peser sur le développement de leurs activités (cas du Groupe Crédit Agricole-Crédit Lyonnais aux USA, de Citigroup ou de Goldman Sachs au Japon...). Ces affaires ont montré que les risques juridiques et d'image sont devenus des risques à part entière parfois aussi douloureux financièrement que les risques de défaillance des contreparties, et pouvant, le cas échéant, menacer l'existence même de l'établissement. En outre, les autorités de supervision nationales ont développé des réglementations plus exigeantes, assorties d'amendes significatives en cas de non respect de ces réglementations. Enfin, le grand public est, de manière croissante, sensibilisé à la nécessité d'une maîtrise des risques et de pratiques éthiques dans le monde des affaires. L'adoption de l'arrêté du 30 mars 2005 s'inscrit donc dans une démarche parfaitement justifiée des autorités françaises, en ligne avec les réflexions actuellement en cours dans les instances internationales, qu'il s'agisse de l'Organisation de coopération et de développement économiques (OCDE) ou du Comité de Bâle, sur le risque de non conformité[2].

Le règlement vise, en cette matière, trois objectifs : souligner l'importance de la maîtrise du risque de non conformité, en préciser le contenu et instaurer, au sein des entreprises assujetties, une culture de la conformité qui, dans les organisations de grande taille, s'appuie sur un métier, structuré en filière. Ces objectifs sont déclinés en mesures concrètes, principalement : une définition du risque, la nomination d'un responsable conformité, des procédures permettant la centralisation d'informations et l'exercice du contrôle en cette matière, et des obligations de formation.

Le risque de non conformité est défini de manière très large comme étant « le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législative ou réglementaire, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions de l'organe exécutif prises notamment en application des orientations de l'organe délibérant ». Si les textes dont il convient de surveiller le respect sont ceux du domaine bancaire et financier (ce qui exclut, par exemple,

les questions fiscales ou sociales, bien qu'un risque de réputation puisse naître dans ces domaines-là également), il n'y a guère de limites, en revanche, dans cette sphère, puisqu'au-delà de la réglementation, doivent bien être prises en compte tant les normes applicables dans la profession, et notamment en matière de déontologie, que les instructions propres à l'établissement. Dans les groupes de taille européenne ou internationale, doivent également être prises en compte les règles des pays où le groupe est présent, à travers des filiales ou des succursales, pour ses activités dans ces pays. Le règlement promeut ainsi une approche globale du risque de non conformité, et insiste sur l'implication de tous, notamment de l'organe délibérant (conseil d'administration, conseil de surveillance, assemblée des associés), dans sa maîtrise.

Un responsable de la conformité doit être nommé : c'est là une innovation majeure. L'ancienne règle de 1997 assignait bien au contrôle interne parmi ses buts 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 » : aujourd'hui, non seulement le risque et les obligations sont plus précisément définis, mais ce rôle est érigé en fonction à part entière. Cette fonction, lorsque l'importance des activités le justifie, doit être structurée en une véritable filière autonome de contrôle, dont le responsable de la conformité est la tête et qui dispose d'agents non seulement dans les services centraux, mais le cas échéant locaux, ainsi que de correspondants dans les unités opérationnelles. L'importance et la particularité de la tâche du responsable de la conformité sont soulignées par l'obligation d'informer l'autorité de contrôle, la Commission bancaire, de sa nomination. Il doit bénéficier d'une certaine indépendance et, lorsqu'il n'est pas membre de l'organe exécutif, il ne doit effectuer aucune opération commerciale, financière ou comptable. Il rapporte directement, selon la configuration retenue, soit au responsable du contrôle permanent, soit à l'organe exécutif : si l'organe exécutif ou l'organe délibérant l'estiment nécessaire, il rend également compte directement à l'organe délibérant. Ainsi, les entreprises assujetties bénéficient-elles d'une certaine marge de manœuvre dans l'organisation du contrôle de conformité, afin de l'adapter à leur taille, leur activité et leur structure de risques.

La fonction conformité se veut préventive, et son responsable doit être en mesure d'exercer un contrôle continu. Le nouveau règlement prévoit la mise en place de procédures d'approbation préalable systématique, incluant un avis écrit de ce responsable ou de l'un des agents qu'il habilite, pour tout nouveau produit, ou pour les transformations significatives apportées aux produits de l'établissement. En outre, il impose l'adoption de procédures de contrôle des opérations réalisées. Enfin, est instaurée la faculté, pour tout dirigeant ou tout agent, de faire part à ce responsable de ses interrogations sur tout dysfonctionnement éventuel dans le respect des obligations de conformité, suivant des procédures

d'information portées à la connaissance de l'ensemble du personnel. Ces procédures d'alerte ainsi que de mise en œuvre des actions visant à remédier à ces dysfonctionnements font l'objet d'examens réguliers de pertinence et de suivi.

Le règlement vise donc à diffuser une culture de conformité au sein des établissements. Au-delà de la désignation d'un responsable dédié, il impose aux entreprises assujetties à la fois une réflexion visant à définir les actions les plus concernées et une obligation de formation du personnel, prioritairement en relation avec ces actions. Par l'implication des dirigeants (et de l'organe délibérant), la mise en place du dispositif de maîtrise du risque de non conformité constitue, pour les entreprises assujetties, l'occasion d'une réflexion stratégique sur leurs activités, leurs risques et leurs procédures de contrôle.

## Le risque d'externalisation

Le recours croissant à l'externalisation s'inscrit dans une logique de recentrage des établissements financiers sur leur cœur de compétences, devant leur permettre d'accroître leur rentabilité tout en demeurant en phase avec les évolutions techniques. Ainsi, ces entreprises font, de manière croissante, appel à des prestataires extérieurs pour les assister dans les fonctions de marketing, comptabilité, informatique... Le développement de ces pratiques, qui conduit des entreprises non soumises directement à la surveillance prudentielle à intervenir dans le processus de réalisation d'opérations bancaires et financières, n'est pas exempt de risques juridiques (contrats imprécis ou incomplets), de réputation (absence de maîtrise de la relation avec le client), stratégiques (perte de compétences) et opérationnels (en cas d'absence de plan de sauvegarde). Il est important, pour la stabilité du système financier et la confiance du public, que cette externalisation de fonctions ne se traduise pas par une externalisation non contrôlée des risques.

Ainsi se justifie l'intérêt des régulateurs pour les procédures d'externalisation : certains pays ont adopté des réglementations spécifiques (Royaume-Uni, Allemagne, Pays-Bas), et des réflexions ont eu lieu au sein d'instances européennes et internationales (Comité européen des superviseurs bancaires - CEBS[3], Comité de Bâle). Le nouveau règlement n° 97-02 vise à donner un cadre à cette externalisation et, de ce fait, à trouver un équilibre entre exigence d'efficacité microéconomique et nécessité de stabilité macroéconomique.

Le nouveau dispositif vise à maintenir la maîtrise de l'entreprise assujettie sur les « activités pour lesquelles elle confie à un tiers, de manière durable et à titre habituel, la réalisation de prestations essentielles » par sous-traitance, démarchage ou par toute autre forme.

Ces prestations essentielles sont les opérations de banque, telles que définies à l'article L. 311-1 du Code monétaire et financier, les services d'investissement (relevant du L. 321-1) pour lesquels l'établissement a été agréé, certaines opérations et services connexes[4], ainsi que « les prestations participant directement à l'exécution » de ces opérations ou services. Il est précisé que, pour ces opérations, les

entreprises assujetties ne peuvent externaliser « toute prestation qui concourt de façon substantielle à la décision engageant l'entreprise vis-à-vis de sa clientèle à conclure une opération » qu'auprès de personnes agréées (ou habilitées selon les normes de leur pays) à effectuer de telles activités. Concrètement, en France, on peut imaginer qu'une banque, dans le cadre de l'instruction de dossiers de crédit, puisse, par exemple, confier le *scoring* à une entreprise spécialisée, mais la banque doit rester maître de la décision d'octroyer ou non le crédit. L'entreprise spécialisée ne saurait ni signer, ni engager le crédit, à moins qu'elle ne soit elle-même établissement de crédit. L'externalisation totale d'activités auprès d'autres entités bancaires est déjà assez répandue au sein d'un même groupe bancaire : on observe même dans certains groupes bancaires l'existence de filiales sans personnel.

Le nouveau règlement prévoit également que le contrôle de l'externalisation s'étend à une autre catégorie de « prestations essentielles », concernant certaines opérations ou services connexes aux opérations bancaires et aux services d'investissement[5], ainsi qu'à toute prestation de services « présentant un effet significatif sur la maîtrise des risques ». Des exemples de cette dernière catégorie peuvent certainement être trouvés dans l'externalisation des services informatiques ou de recouvrement. Mais cette dernière notion reste à l'appréciation des établissements, en fonction de l'intégralité ou de la centralité de ce qui est transféré, sous réserve des observations éventuelles de l'autorité de contrôle. Ces opérations peuvent cependant être externalisées auprès d'entreprises qui ne sont pas elles-mêmes des établissements de crédit ou des entreprises d'investissement.

L'externalisation de toute prestation essentielle, qu'elle soit faite auprès d'un établissement agréé (ou habilité) ou non, est encadrée par le règlement. En effet, pour que l'entreprise assujettie conserve l'entière maîtrise de son activité, l'externalisation doit notamment être formalisée par un contrat écrit permettant de s'assurer d'un certain niveau de qualité de la prestation, d'exigences de *reporting*, de l'existence de mécanismes de secours en cas de difficulté grave affectant la continuité du service, et de l'accès à l'information et au contrôle sur place (« droit de suite »). Lorsque de telles dispositions ne figurent pas dans les contrats en cours à durée indéterminée, elles doivent être introduites au plus tard au 1er janvier 2007. D'autre part, l'organe délibérant doit être informé périodiquement des activités externalisées, de leur déroulement et des risques afférents.

L'externalisation de prestations autres que les prestations essentielles n'est pas visée par le règlement. Par conséquent, il est possible aux entreprises d'y avoir recours sans prescriptions particulières, sous réserve des autres dispositions de la réglementation et des observations éventuelles de l'autorité de contrôle.

## L'articulation des contrôles permanent et périodique

Le contrôle met en œuvre deux démarches complémentaires : d'une part, une surveillance continue des opé-

rations effectuées (contrôle permanent), d'autre part, des audits réalisés ponctuellement (contrôle périodique) qu'il convient, afin d'en assurer la pleine efficacité, de distinguer. En particulier, l'importance que doivent prendre dans l'organisation des grands groupes les différentes filières de contrôle (conformité, suivi et mesure des risques, système de documentation et d'information) rend nécessaire d'assurer une indépendance entre les agents chargés de mettre en œuvre le contrôle permanent et ceux qui doivent en évaluer l'efficacité. En la matière, le règlement apporte des précisions bienvenues sur l'organisation et l'articulation de ces deux formes de contrôle, permettant une harmonisation des pratiques au sein des établissements de la place.

Le contrôle permanent couvre la conformité, la sécurité et la validation des opérations réalisées, le respect des diligences liées à la surveillance des risques associés aux opérations. Le contrôle périodique s'attache à la vérification de la conformité des opérations, du respect des diverses procédures prévues et du niveau de risque effectivement encouru.

La responsabilité du contrôle permanent peut être confiée à une ou à plusieurs personnes. Dans le cas d'un unique responsable, ce dernier peut, le cas échéant, se voir rattacher une pluralité de responsables qui lui rapportent (par exemple, un responsable des risques et un responsable de la conformité rapportant au responsable du contrôle permanent). Dans le deuxième cas, les différents responsables rapportent directement à l'organe exécutif (par exemple, comme on l'a vu, le responsable de la conformité peut être indépendant), dont un membre assure alors directement la cohérence et l'efficacité des différentes tâches de contrôle. Dans tous les cas, la responsabilité ultime du contrôle interne incombe à l'organe exécutif auquel rapportent le ou les différents responsables. La nomination du ou des responsables du contrôle permanent ainsi que celle du responsable unique du contrôle périodique font l'objet d'une obligation d'information de l'organe délibérant et de communication à l'autorité de contrôle.

Les entreprises doivent organiser leurs activités et leur contrôle permanent « de manière à assurer une stricte indépendance entre les unités chargées de l'engagement des opérations et les unités chargées de leur validation, notamment comptable, de leur règlement ainsi que du suivi des diligences liées à la surveillance des risques ». Dès lors que la taille de l'établissement justifie la désignation d'équipes affectées au contrôle permanent, les agents en charge de ce contrôle au niveau central doivent exercer leurs fonctions de manière totalement dédiée, alors que ceux ayant cette charge au niveau local pourront, selon la nature de leur contrôle, exercer également ou non des activités opérationnelles. Par exemple, les responsables risques de structures où sont isolés des risques spécifiques ne pourront exercer de fonctions polyvalentes, alors que les personnes chargées de l'accueil de la clientèle dans les agences pourront également effectuer des contrôles de premier niveau.

Les entreprises doivent également organiser le contrôle périodique de sorte que les agents effectuant les enquêtes, que ce soit au niveau central ou le cas

échéant local, soient nécessairement différents de ceux chargés d'assurer le contrôle permanent et indépendant des entités ou services qu'ils contrôlent. Globalement, les établissements ont une certaine latitude quant à l'architecture de contrôle adéquate en fonction de leur activité, sous réserve des observations de l'autorité de contrôle.

## LES ÉVOLUTIONS RÉCENTES DU CONTEXTE DE LA RÉGLEMENTATION

Les principales nouveautés apportées par l'arrêté du 30 mars 2005, qui complètent le dispositif instauré en 1997, se traduisent pour les assujettis par un ensemble d'obligations nombreuses et détaillées. Des représentants de la profession bancaire et financière ont, d'ailleurs, fait part de leurs préoccupations face aux nouvelles procédures à mettre en place et au travail de suivi qui en découle. Cependant, la légitimité de la démarche n'a jamais été contestée. Pourquoi ? Parce que cette réforme intervient dans un contexte de besoin accru de contrôles, ressenti par tous, nécessitant de nouvelles modalités en complément des formes plus traditionnelles. Quatre évolutions récentes me paraissent très significatives de ce nouveau contexte.

### La maîtrise interne des risques

La réglementation prudentielle met de plus en plus l'accent sur la maîtrise interne des risques et notamment du risque opérationnel.

Cette évolution traduit la prise en compte, par le régulateur, de la complexité croissante des opérations menées par les établissements financiers et la volonté de favoriser la diffusion d'une culture de gestion des risques au sein même de ces structures.

Les nouvelles règles de solvabilité, dites de Bâle II, illustrent parfaitement cette démarche ; d'une part, elles posent une nouvelle exigence de fonds propres relative aux risques opérationnels, s'ajoutant à celles relatives aux risques de marché ou de crédit. Il s'agit du « risque de perte directe ou indirecte résultant de procédures internes inadéquates ou défaillantes, du personnel, des systèmes ou d'événements extérieurs ». Dans ce cadre, la rigueur des procédures et le contrôle de leur stricte application revêt donc une importance primordiale, y compris (et peut-être même surtout) quand elle est externalisée (à cet égard, les plans de continuité revêtent une grande importance). D'autre part, le choix pour les établissements financiers, ouvert par la nouvelle réglementation, de retenir des méthodes internes pour l'appréciation de leurs risques les oblige à détailler par ligne de métier des outils de gestion, de mesure des risques, de *reporting* et de contrôle, non plus en fonction du statut des contreparties (États, banques, entreprises, particuliers...), mais de la nature des risques encourus, au vu d'éléments internes (historiques de pertes) ou externes (notation). Ces systèmes de suivi interne des risques doivent, naturellement, être validés par l'autorité de contrôle : celle-ci est amenée ainsi à accorder autant d'importance aux systèmes de suivi des risques mis en place par les banques qu'aux risques

qu'elles encourent : autrement dit, le qualitatif progresse à côté du quantitatif. Cette nouvelle réglementation responsabilise incontestablement les banques et les conduit à repenser leur organisation et à rapprocher les fonctions financières et les fonctions de contrôle, en donnant une place accrue à ces dernières.

## L'importance de la gouvernance

Dans le secteur bancaire et financier, la gouvernance revêt une importance toute particulière, en raison des puissantes externalités de ce secteur envers l'ensemble de l'économie. La gouvernance est ici d'une importance majeure pour la stabilité financière, qui constitue un bien public. Une bonne connaissance, par les dirigeants des banques, de leurs activités, de leurs résultats et de leurs éventuelles fragilités améliore la capacité des établissements à réagir aux chocs.

De nombreuses instances, nationales ou internationales, ont conduit des travaux sur ce sujet qui ont débouché sur des principes ou des lignes directrices auxquels il est recommandé à toute entreprise de satisfaire. En juillet 2005, le Comité de Bâle a publié un nouveau projet de recommandation en matière de gouvernance spécifique aux établissements de crédit (projet abouti, mais qui attend une approbation formelle du Comité[6]). À travers les huit grands principes affichés, l'insistance est mise sur la transparence interne du fonctionnement des banques : il doit comprendre notamment des chaînes de responsabilités, claires et compréhensibles par tous, à commencer par les organes de direction et de surveillance ; la Direction générale doit être en mesure d'assurer une supervision appropriée des activités et des objectifs, notamment par une politique de revue des objectifs, des limites et des risques, y compris des risques de conformité, en particulier dans les montages juridiquement complexes, voire utilisant des véhicules opaques. Les administrateurs, dont certains doivent être indépendants, doivent être également en mesure d'assurer leur part de contrôle : l'existence d'un comité d'audit est recommandée, du moins pour les grandes banques, ainsi que le recours ponctuel à des audits externes. De nombreuses dispositions nouvelles de la réglementation française font écho à ces recommandations, ainsi qu'aux recommandations du Comité de Bâle relatives à la conformité, publiées en mars 2005.

## Les dégâts du risque de réputation

Quelques affaires retentissantes ont souligné les dégâts irrémédiables du risque de réputation lorsqu'il se déclare.

L'exemple le plus récent, mais aussi particulièrement éclairant, en est offert par Refco : le dirigeant de cette entreprise d'investissement avait dissimulé une importante dette contractée auprès de Refco par une société qu'il contrôlait personnellement, sans doute pour couvrir ses pertes, reportées d'année en année pendant plusieurs exercices consécutifs grâce à un habillage comptable au moment des arrêtés. La découverte de ce montage frauduleux par un

nouvel auditeur interne (en raison d'un contrôle renforcé mis en place parallèlement à l'introduction en Bourse ?) et son annonce par le conseil d'administration, le 10 octobre 2005, a déclenché une crise de confiance qui a très rapidement conduit à un éclatement de ce Groupe de taille internationale et, selon le cas, à un rachat de branches d'activité ou de portefeuilles ou bien à une fermeture (la filiale française, qui avait le statut d'entreprise d'investissement et dont les clients se sont retirés rapidement provoquant l'arrêt quasi total des activités, a vu l'autorisation de retrait de son agrément donnée le 20 décembre 2005). Il n'y avait pourtant pas de péril financier immédiat, puisqu'à l'annonce de cette dette, le dirigeant en cause a été en mesure de contracter un prêt de montant équivalent auprès d'une banque étrangère et a donc débouclé l'opération avec la société qu'il dirigeait. Il s'agit bien là, fondamentalement, des effets dévastateurs d'un manque de gouvernance et d'un défaut répété de contrôle interne (et externe aussi, car les comptes avaient été plusieurs fois certifiés) qui ont conduit à la perte de confiance brutale dans un groupe qui avait pourtant acquis une bonne réputation d'expérience professionnelle.

### La sécurisation juridique de la relation avec la clientèle

Alors que la protection des consommateurs dans le domaine des services financiers se développe, ainsi que la vigilance des associations qui les représentent, la qualité à la fois des produits et de l'information qui accompagne leur vente doit faire l'objet d'une attention soutenue de la part des établissements émetteurs ou distributeurs, comme le montrent certaines affaires récentes dans lesquelles le défaut d'information et des pratiques de distribution inappropriées par rapport à la clientèle relatives à des produits à garantie de performance ont été mis en évidence. Le responsable de la conformité, que le règlement n° 97-02 modifié met en place, est appelé à jouer, à cet égard, un rôle important à travers l'avis qu'il doit formellement porter sur les nouveaux produits de son établissement. La conformité doit être également strictement respectée dans les opérations de conseil en cas d'appel au marché.

Mais les établissements financiers doivent, en sens inverse, se montrer aussi particulièrement soucieux de la qualité de leur clientèle car, à défaut de procédure de contrôle adaptée, ils encourent un risque de sanction de l'autorité de contrôle en matière de non respect des obligations de vigilance antiblanchiment. L'atteinte à la réputation et à l'image peut être très préjudiciable dans ce domaine et dans celui de la lutte contre le financement du terrorisme. Les activités de gestion privée ou de transfert de fonds sont, à cet égard, des activités à risque.

## LA MISE EN ŒUVRE DES NOUVELLES EXIGENCES

Lors des réunions de concertation préalables à l'examen par le CCLRF de l'arrêté renforçant les obligations de contrôle interne, ainsi également que lors de la séance du Comité, de

nombreuses observations ont été formulées, dont il a été largement tenu compte. Néanmoins, il ressortait que ces exigences nouvelles, pour fondées qu'elles soient, d'une part, entraînaient un surcroît de procédures, qui peut avoir un coût non négligeable, et, d'autre part, pouvaient réserver quelques difficultés de mise en œuvre.

## Adaptation de la réglementation selon la taille ou l'activité

Le règlement prévoit des adaptations en fonction de la taille de l'établissement considéré ou de la spécificité de son activité.

La mise en place de cette nouvelle réglementation se traduit par des coûts d'adaptation des structures ou des pratiques. La définition de nouvelles responsabilités, comme la conformité et le suivi des activités externalisées, et les clarifications souhaitées relativement à la séparation des contrôles permanent et périodique, entraînent, en effet, dans de nombreux établissements, des redéfinitions ou des créations de postes, voire un besoin d'embauche additionnel. Les coûts d'information et de formation du personnel seront également importants. L'effort ainsi demandé aux entreprises assujetties varie cependant en fonction de leur activité et de leur taille, les plus grands établissements étant mieux à même de supporter une augmentation, même temporaire, de coûts fixes.

En conséquence, l'arrêté modifiant le règlement n° 97-02 prévoit de nombreuses possibilités d'adaptation, tenant compte de la nature des activités et de leurs risques et de la taille des établissements assujettis. C'est ainsi que, pour les établissements affiliés à un organe central ou ceux appartenant à un groupe bancaire, certaines fonctions de contrôle peuvent être réalisées par d'autres entités du groupe. Lorsque la taille ne justifie pas la dualité, la responsabilité du contrôle de conformité peut être confiée au responsable du contrôle permanent. Enfin, le texte prévoit la possibilité pour de petits établissements d'externaliser certaines fonctions de contrôle (contrôle périodique, effectué par des cabinets d'audit, ou contrôle de la conformité, par recours à des cabinets de conseil juridique), sous leur entière responsabilité et sous le contrôle de la Commission bancaire.

Pour les entreprises d'investissement en particulier, qui sont souvent de petite taille et qui, de surcroît, doivent aussi répondre aux exigences posées par l'Autorité des marchés financiers (AMF), les fonctions de responsable du contrôle permanent et de responsable du contrôle des services d'investissement (RCSI) peuvent être exercées par la même personne : les rapports adressés à l'autorité des marchés au titre des obligations qui incombent au RCSI peuvent également servir à l'autorité de contrôle bancaire.

Les coûts de mise en œuvre des nouvelles obligations sont la contrepartie indispensable de la sécurité et de la réputation de la place, dont tous les acteurs bénéficieront globalement et individuellement. Ces nouvelles pratiques, notamment en termes de conformité, ont, en effet, pour objectif d'éviter des coûts induits par le non respect des réglementations, coûts qui peuvent se révéler particulièrement

significatifs. En outre, dans le cadre du ratio de solvabilité Bâle II, la mise en place d'une maîtrise efficace du risque de non conformité peut conduire à limiter les exigences en termes de fonds propres.

Si des adaptations sont prévues pour les établissements de petite taille ou spécialisés, les obligations du règlement n° 97-02 modifié devront également être déclinées en fonction de la grande taille de certains établissements assujettis. Il conviendra, en effet, de veiller à ce que la masse des informations relatives au contrôle puisse être correctement régulée et traitée. À cet égard, certaines précisions ont été apportées pour éviter le risque selon lequel « trop de contrôle tue le contrôle » : dans le cadre du contrôle périodique, par exemple, lorsque la taille de l'établissement et le nombre de rapports le justifient, peuvent être communiquées à l'organe exécutif (et, s'il le demande, à l'organe délibérant ou au comité d'audit) seulement les conclusions de ces rapports, si elles en reprennent bien les éléments principaux, et non les rapports dans leur totalité.

Globalement, les obligations du règlement devront être croisées avec un mode de gouvernance interne adapté à la taille et permettant un bon équilibre à la fois entre capacité de direction effective et contrôle au niveau de l'organe exécutif et entre organe exécutif et organe délibérant. Bien que lui soit reconnue par le règlement la possibilité, à sa demande, d'être informé des résultats de différents contrôles, l'organe délibérant ne saurait non plus se substituer à l'organe exécutif dans la gestion au quotidien des risques et dans l'adoption de mesures de gestion adaptées aux observations remontant des responsables du contrôle.

## Diversité des normes nationales

Le dispositif de maîtrise du risque de non conformité a notamment pour objectif de sensibiliser plus encore les établissements les plus internationalisés à la nécessité de se conformer à des réglementations nationales parfois diverses.

Le développement international des établissements financiers, par implantation de filiales ou de succursales à l'étranger, conduira sans doute à des difficultés liées à des divergences de normes nationales. Les fonctions de contrôle doivent, en effet, s'exercer au regard d'un référentiel de normes qui ne sont pas seulement les normes du pays d'origine. Les entreprises assujetties doivent s'assurer que leurs implantations à l'étranger mettent en place des dispositifs de contrôle de la conformité respectant à la fois les règles s'appliquant à la maison-mère et les règles locales applicables à leurs activités. Lorsque les règles locales sont plus contraignantes que les règles posées par la réglementation française, ces dernières sont automatiquement réputées satisfaites. Mais il peut se trouver que les dispositions locales fassent échec à l'application des normes françaises : le responsable de la conformité doit alors en être avisé et informer l'autorité de contrôle bancaire. Les responsables de la conformité, qui constitueront autant de relais des bonnes pratiques à l'intérieur des établissements, feront également office

d'interface entre les établissements et les autorités de supervision.

L'acclimatation de l'obligation « d'alerte éthique » (le *whistle blowing* anglo-saxon introduit en particulier dans les obligations de la loi Sarbanes-Oxley) peut également réserver des difficultés d'interprétation ou d'adaptation. Comme indiqué plus haut, l'arrêté introduit, en effet, une obligation de mettre en place une centralisation des informations relatives aux éventuels dysfonctionnements dans la conformité et d'en informer les agents : tout agent se voit donc ouvrir la faculté de faire part de ses interrogations sur ces éventuels dysfonctionnements auprès du responsable de la conformité. Toutefois, à la différence de certains dispositifs américains, il n'y a pas obligation d'alerte (cela reste une faculté pour les agents), ni d'obligation d'alerte d'autorités externes. Après avoir annulé certains dispositifs mis en place dans des sociétés commerciales (contraintes par la loi américaine de le faire), la Commission nationale de l'informatique et des libertés (Cnil) a adopté, le 10 novembre 2005, un document d'orientation définissant un cadre acceptable au regard de la loi française pour ces nouveaux dispositifs internes et relevant que le dispositif prévu par le règlement n° 97-02 modifié ne soulevait pas d'interrogations particulières[7].

L'introduction d'un « droit de suite » (possibilité de contrôles sur place et, le cas échéant, d'inspection de l'autorité de contrôle bancaire française) dans les conventions passées avec les prestataires de services auprès desquels les établissements financiers externaliseront certaines tâches, risque également de susciter des difficultés avec certains cocontractants lorsqu'il s'agit de « délocalisations », dans un référentiel de droit étranger.

Les dispositions relatives au contrôle interne applicables aux établissements de crédit et aux entreprises d'investissement constituent un référentiel important qui met le secteur bancaire et financier français en pointe dans ce domaine, vis-à-vis tant des secteurs bancaires et financiers étrangers que des autres secteurs économiques français. Ces prescriptions ne doivent pas être considérées comme pesantes par ces établissements, mais comme présentant l'avantage de clarifier et d'unifier leurs obligations vis-à-vis à la fois de l'autorité de contrôle, du marché et des tiers : elles instaurent un *level playing field* clair pour l'exercice de « règles de l'art » assez poussées en la matière.

Il est frappant de constater, en comparaison, combien les exigences de contrôle interne, générales ou pour les autres secteurs d'activité, sont encore peu normatives en France. Lorsqu'une société fait appel public à l'épargne, elle a l'obligation légale de joindre au rapport annuel à l'assemblée générale un rapport spécial sur les procédures de contrôle interne mises en place (cette obligation d'information s'applique également à tout établissement financier, mais, hors appel public à l'épargne, au profit de l'organe délibérant, des commissaires aux comptes et de l'autorité de contrôle). Cependant, la réglementation applicable ne renvoie pas à un référentiel et ne détaille donc pas les dispositifs de contrôle interne généralement attendus. L'AMF a,

toutefois, récemment installé un groupe de place chargé de proposer un référentiel de contrôle interne, dont les travaux devraient aboutir avant la fin du 1er semestre 2006. Cet exercice d'autorégulation, qui devrait favoriser une plus grande homogénéité des publications des émetteurs, se double d'une recommandation de l'AMF, à ces derniers, de procéder à l'évaluation de leurs procédures de contrôle interne.

Dans le secteur des assurances, il n'existe pas aujourd'hui de prescriptions relatives à l'organisation du contrôle interne qui relève donc des dispositions prises par chaque établissement, sauf pour ce qui concerne le contrôle interne des placements pour lequel existent des dispositions spécifiques. Un projet de décret, soumis à l'examen du CCLRF en novembre 2005, devrait introduire de nouvelles exigences dans la partie réglementaire du Code des assurances. Toute entreprise d'assurances devra disposer d'un dispositif permanent de contrôle interne. Elle devra également soumettre pour approbation, au moins annuellement, à l'organe délibérant, un rapport décrivant les procédures mises en place, ainsi que leurs objectifs, en insistant notamment sur le contrôle de la conformité des opérations d'assurance à la réglementation et aux orientations internes à l'entreprise. Les procédures doivent permettre de maîtriser les risques liés aux engagements de l'entreprise, les risques liés aux filiales, aux activités externalisées et aux modes de commercialisation, ainsi que les procédures d'élaboration et de vérification de l'information financière et comptable. À travers l'établissement d'un rapport spécifique, qui devra être transmis à l'Autorité de contrôle des assurances et des mutuelles (Acam), ce décret met l'accent sur la transparence des procédures de contrôle interne mises en place, envers les superviseurs et les instances dirigeantes de l'entreprise. Il ne réglemente pas, en revanche, l'organisation du dispositif de contrôle interne de chaque entreprise d'assurances, qui pourra être adaptée à chaque cas particulier, notamment pour tenir compte de la taille de l'entreprise concernée et de la nature de ses activités.

Cependant, quels que soient les garde-fous de la réglementation, la nature ou la quantité de prescriptions, il convient de garder à l'esprit que le contrôle interne repose fondamentalement sur la qualité des dirigeants et de la gouvernance d'entreprise. À cet égard, les affaires Enron, Parmalat et, une nouvelle fois plus récemment, Refco, ont montré que les agissements frauduleux peuvent être d'autant plus longtemps dissimulés qu'ils sont le fait des dirigeants.

Reste néanmoins, sans doute, aussi un besoin de progrès, ainsi que le souligne le Comité de Bâle, dans les diligences relatives au recours à certains fonds, notamment en cas de fort effet de levier où l'attractivité est à la mesure du risque, ou à certains montages : en particulier, l'utilisation d'entités *ad hoc* dans des centres *offshore* mériterait de faire l'objet d'obligations d'information, par exemple dans un rapport annexe au rapport annuel.

## *Notes*

1. La loi de sécurité financière a réorganisé le pouvoir réglementaire en matière de banque et d'assurance. D'une part, le pouvoir réglementaire en matière bancaire et financière était auparavant délégué au CRBF dont les règlements étaient homologués par arrêté du ministre en charge de l'économie avant leur entrée en vigueur. D'autre part, la compétence du ministre en matière de réglementation des assurances était exercée après avis du Conseil national des assurances (CNA). Dans les secteurs de la banque comme de l'assurance, le pouvoir réglementaire est désormais directement exercé par le ministre après avis du CCLRF, qui remplace en conséquence le CRBF et la Commission de la réglementation du CNA.

2. *Compliance and the Compliance Function in Banks,* Banque des règlements internationaux (BRI), avril 2005 (www.bis.org).

3. Cf. *High Level Principles on Outsourcing* (www.c-ebs.org).

4. Visés aux § 1, 2 et 3 de l'article L. 311-2 du Code monétaire et financier (opérations de change, sur or, placement de produits financiers...) et aux § 1, 2 ,5 et 6 de l'article L. 321-2 (conservation ou administration d'instruments financiers...).

5. Visés aux § 4, 5 et 6 de l'article L. 311-2 du Code monétaire et financier (opérations de conseil et d'assistance en gestion financière ou de patrimoine, location simple...) et aux § 3, 4, 7 et 8 de l'article L. 321-2 (conseil, location de coffres-forts...).

6. *Enhancing Corporate Governance for Banking Organisations,* Banque des règlements internationaux (BRI), juillet 2005.

7. Document d'orientation pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978, modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés (www.cnil.fr).