Circulaire de la Commission fédérale des banques : Surveillance et contrôle interne du 27 septembre 2006

Sommaire

I. Objet

La présente circulaire contient les prescriptions relatives au « corporate governance », à la surveillance de l'activité commerciale ainsi qu'au contrôle interne et à sa surveillance par les organismes compétents dans les banques, les négociants en valeurs mobilières, les groupes financiers (art. 3c al. 1 LB) et les conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières (art. 3c al. 2 LB). Ceux-ci sont désignés ci-après par le terme d'« établissements ». **1**

Par contrôle interne (synonyme : système de contrôle interne), on entend l'ensemble des structures et processus de contrôle qui, à tous les échelons de l'établissement, constituent la base de son bon fonctionnement et la réalisation des objectifs de la politique commerciale. Le contrôle interne ne comprend pas uniquement les activités de contrôle a posteriori, mais également celles en rapport avec la gestion et la planification. Un contrôle interne efficace englobe notamment des activités de contrôle intégrées dans les processus de travail, des procédures dédiées à la gestion des risques et au respect des normes applicables (compliance), un contrôle des risques indépendant de la gestion des risques et la fonction compliance. La révision interne vérifie et évalue le contrôle interne et contribue ainsi à son amélioration constante. **2**

II. Champ d'application

La présente circulaire s'applique aux établissements indiqués au chiffre marginal (ci-après Cm) 1, sous réserve des restrictions suivantes : **3**

- Négociants en valeurs mobilières ne bénéficiant pas d'un statut bancaire : les Cm 18-40 ne s'appliquent pas s'il y a identité entre les personnes siégeant au conseil d'administration et celles exerçant la direction opérationnelle. Les Cm 41-53 s'appliquent par analogie. **4**

- Banquiers privés : les Cm 18-40 ne s'appliquent pas. Les Cm 41-53 s'appliquent par analogie. S'agissant des autres dispositions, des dérogations et des simplifications sont admises, en accord avec la société d'audit et l'autorité de surveillance, tant que les partenaires présentent les caractéristiques requises en matière de responsabilité personnelle et de conduite des affaires. **5**

- Filiales de banques, de négociants en valeurs mobilières, sociétés filles principalement actives dans le domaine financier détenues directement ou indirectement par des groupes financiers ou conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières, suisses ou étrangers : les Cm 18-40 ne s'appliquent pas, mais la mise en place d'un comité d'audit est conseillée. Les Cm 41-53 sont applicables par analogie. **6**

- Succursales d'établissements étrangers : les Cm 9-53 ne s'appliquent pas. Les autres dispositions s'appliquent par analogie. **7**

- Entreprises qui ne sont pas principalement actives dans le domaine financier appartenant à des groupes financiers ou des conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières : la circulaire ne s'applique pas. En cas de doute, certaines sociétés du groupe peuvent être expressément exemptées de son application à la demande de la société mère. **8**

III. Conseil d'administration

A. Tâches et responsabilités

a) Surveillance et contrôle interne

Il incombe au conseil d'administration, c'est-à-dire à l'organe exerçant la haute direction, la surveillance et le contrôle, de réglementer, d'instaurer, de maintenir, de surveiller et de valider régulièrement un contrôle interne approprié. Ce dernier doit être adapté à la taille, à la complexité, à la structure et au profil de risque **9**

de l'établissement.

En instaurant un contrôle interne basé sur une analyse systématique des risques et en le surveillant, le conseil d'administration s'assure que tous les risques significatifs auxquels s'expose l'établissement sont identifiés, limités et surveillés. Dans les groupes financiers et les conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières, il convient en particulier de prendre aussi en compte les risques résultant du regroupement de plusieurs entreprises en une entité économique unique. L'analyse systématique des risques doit être documentée par écrit. **10**

Le conseil d'administration doit discuter régulièrement avec la direction de son appréciation sur l'adéquation et de l'efficacité des mesures du contrôle interne. **11**

b) Environnement de contrôle

Par la remise d'instructions à la direction opérationnelle, le conseil d'administration fait en sorte que les collaborateurs de tous les échelons hiérarchiques connaissent et comprennent leurs responsabilités et devoirs dans le processus de contrôle interne. **12**

Le conseil d'administration veille à ce que la pression éventuellement exercée sur les collaborateurs de tout échelon hiérarchique pour la réalisation d'objectifs ne puisse pas conduire à contourner les mécanismes de contrôle. Il fait en sorte que les systèmes de rémunération ne créent aucune incitation au non-respect des mécanismes de contrôle. **13**

Le conseil d'administration fait en sorte que la gestion des conflits d'intérêts soit réglée. Lorsque, dans un cas particulier, un conflit d'intérêts ne peut être évité, l'établissement prend des mesures afin de le gérer. **14**

c) Instauration et surveillance de la révision interne

Le conseil d'administration instaure une révision interne, qui lui est directement subordonnée ou qui est subordonnée au comité d'audit (ou à un autre comité). En ce qui concerne l'organisation, les tâches et les responsabilités ainsi que les obligations de rendre compte et de rapporter, voir Cm 54-79. **15**

Le conseil d'administration ou le comité responsable surveille et juge l'efficacité de la révision interne et s'assure régulièrement que celle-ci dispose de ressources et de compétences appropriées ainsi que de l'indépendance et de l'objectivité adéquates pour assumer ses tâches de contrôle au sein de l'établissement. **16**

B. Membres du conseil d'administration

a) Exigences générales

Pour accomplir ses tâches, le conseil d'administration doit satisfaire, en tant qu'organe, les conditions requises à cet effet, notamment en termes de compétences professionnelles, d'expérience et de disponibilité. Il évalue au moins une fois par an et par écrit les objectifs atteints et son mode de travail. **17**

b) Indépendance

Les membres du conseil d'administration organisent leurs rapports personnels et professionnels de manière à éviter autant que possible les conflits d'intérêts avec l'établissement. En vertu de l'art. 8 al. 2 OB, il est en particulier interdit aux membres du conseil d'administration de faire simultanément partie de la direction opérationnelle de l'établissement. **18**

Le conseil d'administration est composé pour un tiers au moins de membres répondant aux critères d'indépendance énoncés aux Cm 20-24. Les noms de ces membres doivent figurer dans le rapport annuel. Si moins du tiers des administrateurs satisfont aux exigences d'indépendance, une justification doit être fournie dans le rapport annuel. **19**

Un membre du conseil d'administration est réputé indépendant s'il satisfait au moins aux critères suivants : **20**

- il n'occupe pas d'autre fonction dans l'établissement et n'en a pas occupé au cours des deux dernières années; **21**

- il n'a pas occupé, au cours des deux dernières années, la fonction de réviseur responsable de l'établissement au sein de la société d'audit; **22**

- il n'entretient avec l'établissement aucune relation d'affaires qui, par sa nature ou son ampleur, conduit à un conflit d'intérêts, et **23**

- il ne détient pas de participation qualifiée (au sens de l'art. 3 al. 2 let. c^{bis} LB et de l'art. 10 al. 2 let. d LBVM) dans l'établissement, ni ne représente un détenteur d'une telle participation. **24**

Les membres du conseil d'administration de banques cantonales ou communales désignés ou élus par les cantons, communes ou autres corporations de droit public cantonales ou communales qui contrôlent ces établissements sont réputés indépendants au sens du Cm 24 si : **25**

- ils n'appartiennent pas au gouvernement ou à l'administration du canton ou de la commune ni à une autre corporation de droit public communale ou cantonale, et **26**

- ils ne reçoivent pas d'instructions de l'organe qui les a élus relatives à leur activité en tant que membres du conseil d'administration. **27**

C. Répartition des tâches au sein du conseil d'administration et de ses comités

Le conseil d'administration peut instaurer des comités chargés de le seconder ou confier des tâches à certains de ses membres. **28**

Un comité d'audit doit être instauré dès lors que l'établissement atteint une certaine taille ou un certain niveau de complexité (Cm 32-36). **29**

Lorsqu'un établissement ne dispose pas d'un comité d'audit, le conseil d'administration charge un ou deux administrateurs indépendants répondant aux exigences du Cm 39, mais en principe pas le président du conseil d'administration, d'accomplir les tâches définies aux Cm 41-53. L'autorité de surveillance peut octroyer des dérogations. Si les tâches mentionnées sont confiées au président du conseil d'administration, une justification doit être fournie dans le rapport annuel. **30**

Les tâches et compétences déléguées à des comités ou à des personnes, de même que les obligations correspondantes en matière d'information, de coordination et de rapport, doivent être réglées par le conseil d'administration. Dans tous les cas, le conseil d'administration reste collectivement responsable des tâches déléguées. **31**

D. Comité d'audit

a) Critères régissant l'instauration d'un comité d'audit

Les établissements instaurent un comité d'audit (« audit committee ») dès lors qu'au moins un des critères énumérés aux Cm 33-36 s'applique : **32**

- total du bilan > 5 milliards de CHF **33**

- volume des dépôts (portefeuilles de titres et de métaux précieux déposés par les clients, sans les banques, selon le reporting prudentiel AU 001 / AU 101) > 10 milliards de CHF **34**

- fonds propres requis en vertu de l'ordonnance sur les fonds propres (OFR) > 200 millions de CHF **35**

- cotation (titres de participation) **36**

Lorsqu'un établissement s'abstient de créer un comité d'audit bien qu'un ou plusieurs des critères définis aux Cm 33-36 s'appliquent, une justification doit être fournie dans le rapport annuel. **37**

b) Exigences concernant les membres d'un comité d'audit

La majorité des membres doivent satisfaire aux exigences en matière d'indépendance définies aux Cm 20-24; si moins de la moitié des membres satisfont à ces exigences, une justification doit être fournie dans le rapport annuel. **38**

Les membres du comité d'audit disposent de bonnes connaissances et d'expérience en matière financière et comptable et connaissent l'activité de réviseur interne et externe. **39**

Le président du conseil d'administration ne fait en principe pas partie du comité d'audit. Si l'établissement décide qu'il en fait partie, une justification doit être fournie dans le rapport annuel. **40**

c) Tâches d'un comité d'audit

Le comité d'audit peut attribuer des mandats dans le cadre de ses fonctions. **41**

aa) Surveillance et évaluation de l'intégrité des bouclements financiers

Le comité d'audit :

- procède à une analyse critique des bouclements financiers, c'est-à-dire des comptes de l'entreprise et, le cas échéant, du groupe, des comptes annuels et intermédiaires (publiés) ainsi que l'établissement en conformité avec les principes comptables appliqués, et apprécie notamment l'évaluation des principaux postes du bilan et hors bilan; **42**

- discute les bouclements financiers et la qualité des procédures comptables sous-jacentes avec le membre de la direction chargé des finances et de la comptabilité, le réviseur responsable ainsi que le responsable de la révision interne; **43**

- rend compte au conseil d'administration des travaux effectués conformément aux Cm 42-43 et émet une recommandation dans laquelle il indique s'il estime que les comptes peuvent être soumis à l'assemblée des détenteurs du capital. La décision appartient à l'ensemble du conseil d'administration. **44**

bb) Surveillance et évaluation du contrôle interne dans le domaine de l'établissement des rapports financiers

Le comité d'audit :

- surveille et évalue l'adéquation et l'efficacité du contrôle interne dans le domaine de l'établissement des rapports financiers; **45**

- s'assure, en cas de modifications substantielles du profil de risque de l'établissement, que le contrôle interne dans le domaine de l'établissement des rapports financiers est adapté en conséquence. **46**

cc) Surveillance et évaluation de l'efficacité de la société d'audit et de sa coopération avec la révision interne

Le comité d'audit :

- évalue l'analyse des risques, la stratégie d'audit en découlant et le plan d'audit axé sur les risques de la société d'audit, ceci au moins une fois par an et en cas de modifications substantielles du profil de risque de l'établissement (circ.-CFB 05/1 « Audit », annexe 1); **47**

- procède à une analyse critique des rapports d'audit sur l'audit des comptes annuels et l'audit prudentiel (circ.-CFB 05/2 « Rapport d'audit ») et les commente avec le réviseur responsable; **48**

- s'assure que les insuffisances constatées sont corrigées et que les recommandations de la société d'audit sont mises en œuvre; **49**

- évalue les prestations et les rémunérations de la société d'audit et s'assure de leur indépendance; **50**

- évalue la coopération entre société d'audit et révision interne. **51**

dd) Evaluation du contrôle interne qui ne porte pas sur le domaine de l'établissement des rapports financiers et de la révision interne

Le comité d'audit :

- évalue le bon fonctionnement du contrôle interne qui ne porte pas sur le domaine de l'établissement des rapports financiers, notamment la fonction de compliance et le contrôle des risques, dans la mesure où ce jugement n'est pas effectué par d'autres comités du conseil d'administration; **52**

- doit être informé des résultats des contrôles effectués par la révision interne et entretenir des contacts réguliers avec le responsable de cette dernière, même si la révision interne est subordonnée, conformément aux Cm 28 et 31, à l'ensemble du conseil d'administration ou à un autre comité appartenant à ce dernier. **53**

IV. Révision interne

A. Instauration

Chaque établissement est tenu d'instituer une révision interne (cf. art. 9 al. 4 OB et art. 20 al. 2 OBVM). **54**

Dans des cas particuliers, l'autorité de surveillance peut, après consultation de la société d'audit, exempter un établissement de l'obligation prévue au Cm 54. **55**

Lorsque l'instauration d'une révision interne propre à l'établissement n'apparaît pas appropriée, les tâches de révision interne peuvent être confiées à : **56**

- la révision interne de la société mère ou la révision interne d'une autre société du groupe, dans la mesure où il s'agit d'une banque, d'un négociant en valeurs mobilières ou d'un autre intermédiaire financier (par exemple une compagnie d'assurances) soumis à une surveillance étatique (pour les banques étrangères, dans le cadre de l'art. 4^{quinquies} LB), **57**

- une seconde société d'audit indépendante de celle de l'établissement, ou **58**

- un tiers indépendant, à condition que la société d'audit confirme sa qualification professionnelle. **59**

B. Positionnement hiérarchique et organisation

La révision interne est directement subordonnée au conseil d'administration ou à l'un de ses comités et elle exécute les tâches de révision et de surveillance que celui-ci lui confie. La révision interne rend compte prioritairement à l'instance du conseil d'administration à laquelle elle est directement subordonnée. **60**

La révision interne du groupe financier ou du conglomérat financier s'étend au minimum à toutes les entreprises devant être consolidées conformément aux art. 3b-g LB, aux art. 10 al. 5 et 14 LBVM ainsi qu'aux art. 6-10 OFR. Lorsqu'il existe, dans des sociétés du groupe, des départements de révision autonomes, ceux-ci doivent être fonctionnellement subordonnés à la révision interne du groupe financier ou du conglomérat financier. **61**

Le responsable de la révision interne est nommé par le conseil d'administration. **62**

La révision interne travaille indépendamment des processus d'affaires quotidiens. **63**

La révision interne dispose d'un droit de contrôle illimité au sein de l'établissement et de ses entreprises devant être consolidées au sens du Cm 61. Elle a un droit d'accès illimité à tous les livres, documents, procès-verbaux et autres notes, ainsi qu'aux supports de données et systèmes. Tous les renseignements nécessaires à l'accomplissement de ses travaux d'audit doivent être mis à sa disposition. **64**

Les bases nécessaires à la révision interne, telles qu'un règlement précisant son organisation, ses tâches et ses responsabilités, doivent être édictées selon les rapports de subordination directs par le conseil d'administration ou le comité responsable. Pour le reste, la révision interne définit elle-même son mode de travail (par exemple méthodologie, types d'audits, formation et perfectionnement). **65**

La révision interne doit répondre aux exigences qualitatives de l'Association suisse d'audit interne (ASAI). Des dérogations doivent être justifiées dans le rapport annuel. Le travail de la révision interne est fondé sur les « Standards for the Professional Practice » de l'Institute of Internal Auditors (IIA). **66**

La révision interne doit être aménagée en fonction de la taille, de la complexité et du profil de risque de l'établissement et forme, au plan organisationnel, une unité autonome. Elle doit disposer de personnel et de ressources matérielles (par exemple outils informatiques) suffisants pour exécuter son mandat. Dans l'ensemble, les cadres doivent disposer de connaissances approfondies des domaines d'activité dans lesquels l'établissement opère. D'une manière générale, il faut veiller à ce que la régularité de la gestion et l'adéquation du système de contrôle interne soient évaluées par des réviseurs qualifiés. **67**

Le système de rémunération des collaborateurs de la révision interne ne doit pas comprendre d'éléments susceptibles de générer des conflits d'intérêts. En particulier, la rémunération (par exemple salaires, bonus, honoraires et primes) ne doit pas dépendre du résultat de produits ou transactions spécifiques. **68**

C. Tâches et responsabilités

a) Evaluation des risques, planification des révisions et rapports

La révision interne fournit des bases décisionnelles importantes permettant d'apprécier si l'établissement possède un système de contrôle interne efficace et adapté à son profil de risque. **69**

La révision interne procède au moins une fois par an à une évaluation globale des risques encourus par l'établissement, en tenant dûment compte des évolutions externes (par exemple contexte économique, modifications réglementaires) et des facteurs internes (par exemple projets importants, réorientation de l'activité). **70**

Sur la base de cette évaluation des risques, la révision interne fixe les objectifs d'audit principaux de la période d'audit suivante. **71**

En outre, la révision interne veille à ce que toutes les activités de l'établissement comportant un risque soient soumises, dans le cadre d'une planification pluriannuelle, à un audit effectué par elle-même ou par la société d'audit. **72**

La révision interne informe par écrit le conseil d'administration ou le comité responsable et la direction opérationnelle de son évaluation des risques et de ses objectifs d'audit et fait approuver ces derniers, ainsi que la planification de l'audit, par le conseil d'administration ou le comité responsable. Elle distribue à la société d'audit une copie des documents. **73**

Pendant la période d'audit, la révision interne évalue si des modifications substantielles du profil de risque sont intervenues et si celles-ci requièrent un ajustement de la planification de l'audit. Dans l'affirmative, la révision interne soumet en temps utile les modifications substantielles de la planification annuelle au conseil d'administration ou au comité responsable pour approbation. Elle informe la société d'audit de ces changements. **74**

La révision interne rend compte au conseil d'administration ou au comité responsable et à la direction, en temps utile et par écrit, de toutes les constatations importantes effectuées dans le cadre d'un audit. **75**

Au moins une fois par an, la révision interne rédige un rapport écrit sur les résultats essentiels des audits effectués et sur ses principales activités pendant la période et le soumet, avec les conclusions qui en découlent, au conseil d'administration ou au comité responsable pour information. Ce rapport sera également adressé à la direction et à la société d'audit. **76**

En outre, la révision interne informe au moins une fois par semestre le conseil d'administration ou le comité responsable des corrections apportées aux insuffisances constatées et de l'état d'avancement de la mise en œuvre des recommandations de la révision interne et de la société d'audit. La remise de cette information ainsi que le suivi correspondant (« audit tracking ») peuvent être assurés par une autre instance indépendante au sein de l'établissement, par exemple par la fonction de compliance ou le contrôle des risques. **77**

b) Répartition des tâches entre révision interne et société d'audit

La révision interne et la société d'audit coordonnent leurs activités dans le cadre de la détermination de leurs objectifs et stratégies d'audit respectifs. Elles défendent ainsi leurs points de vue respectifs et peuvent fixer sur cette base une approche commune. La révision interne reste responsable de la réalisation de ses objectifs d'audit. **78**

La révision interne communique en temps utile ses rapports à la société d'audit. La société d'audit est en droit de consulter les documents de travail de la révision interne. Inversement, la société d'audit met ses rapports d'audit à disposition de la révision interne. **79**

V. Direction opérationnelle

A. Tâches et responsabilités

La direction opérationnelle met en œuvre les instructions du conseil d'administration en matière d'instauration, de maintien et de suivi régulier du contrôle interne. **80**

La direction opérationnelle :

- élabore des procédures appropriées pour identifier, mesurer, évaluer, analyser et contrôler les risques pris par l'établissement. La concrétisation des activités de contrôle intégrées dans les processus de travail conformément aux Cm 87-96, la fonction de compliance définie aux Cm 100-112 et le contrôle des risques prévu aux Cm 113-125 en font en particulier partie; **81**

- met en place et documente une structure d'organisation qui définit clairement les responsabilités, compétences, obligations de rendre compte, pouvoirs d'injonction et de décision ainsi que les flux d'informations; **82**

- veille à ce que toutes les informations importantes sur l'évolution de l'entreprise soient collectées, distribuées et traitées (système de gestion de l'information); **83**

- vérifie régulièrement l'adéquation du contrôle interne; **84**

- rend périodiquement compte au conseil d'administration de l'efficacité du contrôle interne et l'informe, ainsi que la révision interne, immédiatement en cas de constatations graves. **85**

B. Séparation des fonctions et activités de contrôle

La direction opérationnelle veille à une séparation appropriée des fonctions et évite l'attribution de responsabilités conflictuelles. Dans les cas où une séparation des fonctions ne peut pas être entièrement réalisée en raison de la taille de l'entreprise, elle attache une importance particulière à un renforcement conséquent de la responsabilité de conduite des instances hiérarchiques. **86**

Des activités de contrôle, qui font partie intégrante de l'ensemble des processus de travail, sont prévues, par exemple sous forme de : **87**

- contrôles de déroulement : ceux-ci constatent les écarts par rapport aux objectifs à un moment où des corrections sont encore aisément réalisables; **88**

- contrôles de résultat : ceux-ci comparent les objectifs fixés aux résultats effectivement atteints. Ils sont utilisés lorsque qu'il n'est plus nécessaire et/ou plus possible d'apporter directement des corrections; **89**

- vérifications de comportement : celles-ci sont utilisées pour vérifier le comportement d'individus ou d'unités organisationnelles. Elles sont notamment mises à contribution lorsqu'aucun résultat quantitatif ne peut être observé. **90**

Les activités de contrôle applicables sont notamment les suivantes : **91**

- contrôles d'activités : des rapports adaptés au niveau hiérarchique sur la performance économique et la situation en matière de risques et de contrôle doivent être régulièrement remis aux différents échelons de fonctions, qui les soumettent à un regard critique; **92**

- contrôles physiques : par exemple sous forme de l'application du principe des quatre yeux, de limitation de l'accès technique au numéraire et aux objets de valeur, d'inventaires périodiques; **93**

- vérification du respect des limites prescrites; **94**

- vérification du respect des compétences et autorisations, en particulier des autorisations relatives à l'accès aux systèmes informatiques et aux données de base, ainsi qu'à leurs mutations (« golden-keyholders »); **95**

- vérification et contrôles de concordance, par exemple de transactions et de positions comptables. **96**

C. Compliance (respect des normes)

On entend par compliance la conformité aux prescriptions légales, réglementaires et internes, ainsi que le respect des normes et règles déontologiques en usage sur le marché concerné. **97**

Le risque de compliance correspond au risque de manquements aux prescriptions, normes et règles et aux sanctions légales et réglementaires, pertes financières ou atteintes à la réputation qui peuvent en découler. **98**

Il incombe à la direction opérationnelle de mettre en place des systèmes et des processus internes appropriés pour assurer la compliance au sein de l'établissement. A cet effet, elle prend toutes mesures et dispositions opérationnelles requises, veille notamment à ce qu'un ensemble adéquat d'instructions soit établi et organise l'implication de tous les collaborateurs, à tous les échelons, dans le maintien de la compliance. Dans les établissements opérant à l'échelle internationale, il convient en particulier de s'assurer que les instructions produisant effet dans plusieurs pays soient compatibles avec le droit local. **99**

D. Fonction de compliance

a) Instauration et positionnement hiérarchique

Chaque établissement se dote d'une fonction de compliance qui, dans le cadre de sa mission, dispose d'un droit illimité à l'information, à son accès et à sa consultation. La fonction de compliance est intégrée dans l'organisation globale de l'établissement, mais indépendante de ses activités opérationnelles génératrices de revenus. **100**

La fonction de compliance doit disposer de ressources et de compétences adaptées à la taille de l'établissement, à la complexité de son activité et de son organisation et à son risque de compliance. **101**

L'établissement désigne un membre de la direction comme responsable de la fonction de compliance et fait ainsi en sorte que cette dernière puisse accéder librement à la direction. **102**

Le système de rémunération des collaborateurs de la fonction de compliance ne doit pas comprendre **103**

d'éléments susceptibles de générer des conflits d'intérêts. En particulier, la rémunération (par exemple salaires, bonus, honoraires et primes) ne doit pas dépendre du résultat de produits ou transactions spécifiques.

Lorsqu'il n'existe pas de conflits d'intérêts, la fonction de compliance peut constituer un département avec d'autres fonctions internes, par exemple avec le service juridique ou le contrôle des risques. Les tâches de chaque fonction doivent toutefois être clairement définies et attribuées. **104**

En particulier dans les établissements dont l'activité et l'organisation sont peu complexes et le risque de compliance faible, la fonction de compliance peut être assurée par des collaborateurs travaillant à temps partiel ou employés parallèlement à une autre fonction interne avec laquelle il n'existe pas de conflits d'intérêts. Elle peut également être assurée dans le cadre d'un contrat d'externalisation. **105**

Dans les petits établissements où l'intégration et l'indépendance de la fonction de compliance requises au Cm 100 et l'absence de conflits d'intérêts exigée au Cm 105 ne peuvent pas être entièrement garanties pour des raisons de taille, les tâches incombant à la fonction de compliance doivent être accomplies de manière fiable par un autre biais. Il appartient à la société d'audit d'en juger et de prendre position dans le rapport sur l'audit prudentiel. **106**

b) Tâches et responsabilités

Les tâches, les responsabilités et l'obligation de rapporter incombant à la fonction de compliance doivent être fixées dans une réglementation approuvée par la direction ou le conseil d'administration. **107**

En règle générale, les tâches de la fonction de compliance comprennent :

- l'appui et le conseil à la direction opérationnelle et aux collaborateurs en matière d'application et de surveillance de la compliance; **108**

- au moins une fois par an, l'évaluation du risque de compliance lié à l'activité de l'établissement et l'élaboration d'un plan d'action axé sur le risque, plan qui doit être approuvé par la direction opérationnelle. Le plan d'action doit aussi être mis à disposition de la révision interne; **109**

- l'appui à la direction opérationnelle en matière de formation et d'information des collaborateurs en matière de compliance; **110**

- la remise à la direction, en temps utile, de rapports sur les modifications importantes de l'évaluation du risque de compliance, les manquements graves constatés en matière de compliance et les enquêtes menées à ce sujet ainsi que l'appui fourni à la direction opérationnelle lors du choix des instructions à donner ou des mesures à prendre. La révision interne doit en être informée; **111**

- la remise au conseil d'administration d'un rapport annuel sur l'évaluation du risque de compliance et l'activité de la fonction de compliance telle que définie aux Cm 108-111. Une copie du rapport doit être aussi mise à disposition de la révision interne et de la société d'audit. **112**

E. Contrôle des risques

a) Instauration et positionnement hiérarchique

Chaque établissement se dote d'un contrôle des risques qui, dans le cadre de sa mission, dispose d'un droit illimité à l'information, à son accès et à sa consultation. Le contrôle des risques est intégré dans l'organisation globale de l'établissement mais indépendant de ses activités opérationnelles génératrices de revenus. **113**

Le contrôle des risques doit disposer de ressources et de compétences adaptées à la taille de l'établissement, à la complexité de son activité et de son organisation et à son profil de risque. **114**

L'établissement désigne un membre de la direction opérationnelle en tant que responsable du contrôle des risques et fait ainsi en sorte que le contrôle des risques puisse accéder librement à la direction. **115**

Selon les différentes catégories de risques auxquels est exposé l'établissement (par exemple risques de marché, de crédit, opérationnels), le contrôle des risques peut être constitué de plusieurs départements ou fonctions indépendants, qui rendent toutefois tous compte au membre de la direction responsable du contrôle des risques. **116**

Le système de rémunération des collaborateurs du contrôle des risques ne doit pas comprendre d'éléments susceptibles de générer des conflits d'intérêts. En particulier, la rémunération (par exemple salaires, bonus, honoraires et primes) ne doit pas dépendre du résultat de produits ou transactions spécifiques. **117**

Lorsqu'il n'existe pas de conflits d'intérêts (par exemple avec la fonction de compliance), le contrôle des risques peut constituer un département avec d'autres fonctions internes. Les tâches de chaque fonction doivent toutefois être clairement définies et attribuées. **118**

En particulier dans les établissements dont l'activité et l'organisation sont peu complexes et le risque faible, le contrôle des risques peut être assuré par des collaborateurs travaillant à temps partiel ou employés parallèlement à une autre fonction interne avec laquelle il n'existe pas de conflits d'intérêts. **119**

Dans les petits établissements où l'intégration et l'indépendance du contrôle des risques requises au Cm 113 et l'absence de conflits d'intérêts exigée au Cm 119 ne peuvent pas être entièrement garanties pour des raisons de taille, les tâches incombant au contrôle des risques doivent être accomplies de manière fiable par un autre biais. Il appartient à la société d'audit d'en juger et de prendre position dans le rapport sur l'audit prudentiel. **120**

b) Tâches et responsabilités

Les tâches, les responsabilités et l'obligation de rapporter incombant au contrôle des risques doivent être fixées dans une réglementation approuvée par la direction opérationnelle ou le conseil d'administration. **121**

Le contrôle des risques surveille, en tant que fonction de contrôle indépendante, le profil de risque pris par l'établissement. Il fournit les informations nécessaires à la surveillance des risques et élabore les bases fondant la politique de risque de l'entreprise (« risk policy »), sa propension au risque (« risk appetite ») et les limites de risque qui doivent être approuvées par la direction opérationnelle ou le conseil d'administration. **122**

Il incombe notamment au contrôle des risques d'aménager et de mettre en place des systèmes de surveillance des risques adéquats et de les adapter en fonction des nouvelles affaires et des nouveaux produits, de définir et d'appliquer des bases et des méthodes pour la mesure des risques (par exemple méthodes d'évaluation et d'agrégation, validation de modèles) et de surveiller les systèmes appropriés utilisés pour prendre en compte les dispositions en matière de fonds propres, de répartition des risques et de liquidités. **123**

Le contrôle des risques remet au moins une fois par semestre un rapport à la direction opérationnelle relatif aux risques et aux positions-risque. En cas d'évolution particulière de la situation, il en informe immédiatement la direction opérationnelle et la révision interne. **124**

Au moins une fois par année, le contrôle des risques présente au conseil d'administration un rapport sur les risques encourus par l'établissement et sur son activité telle que définie aux Cm 122-124. Une copie du rapport doit être aussi mise à disposition de la révision interne et de la société d'audit. **125**

c) Délimitation par rapport à la gestion des risques

La gestion des risques a pour but la gestion et la restriction complètes et systématiques des risques sur la base de connaissances économiques et statistiques. Elle comprend l'identification, la mesure, l'évaluation, la gestion et l'établissement de rapports sur des positions-risque individuelles ou agrégées. La gestion des risques est assurée, aux niveaux organisationnels appropriés, au moyen de méthodes adéquates qui tiennent compte des particularités de l'établissement. **126**

VI. Audit et évaluation par la société d'audit

Les sociétés d'audit vérifient le respect de la présente circulaire conformément à la circ.-CFB 05/1 « Audit » et consignent le résultat de leurs travaux d'audit dans le rapport d'audit (circ.-CFB 05/2 « Rapport d'audit »). **127**

VII. Entrée en vigueur

Date d'entrée en vigueur : 1er janvier 2007. **128**

Remplace la circ.-CFB 95/1 « Révision interne » du 14 décembre 1995 et les directives pour le contrôle interne de l'ASB de juin 2002. **129**

VIII. Dispositions transitoires

Les établissements doivent se mettre en conformité avec les dispositions de la présente circulaire d'ici au 1er janvier 2008 au plus tard. S'agissant des exigences relatives à l'indépendance du conseil d'administration et du comité d'audit, un délai transitoire est accordé jusqu'au 1er janvier 2009. **130**

Bases légales :

- LB : art. 3 al. 2 let. a; art. 3b-h; art. 4quinquies
- OB : art. 8 al. 2, art. 9; art. 44 let. o
- OFR : art. 6-11
- LBVM : art. 10 al. 2 let. a; al. 5; art. 14
- OBVM : art. 19; art. 20; art. 26; art. 29 al. 1
- OBVM-CFB : art. 8 al. 1