Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

# Circulaire 2016/xx
# Gouvernance d'entreprise – banques

## Gouvernance d'entreprise, gestion des risques et contrôles internes des banques



| | |
|---|---|
| Référence : | Circ.-FINMA 16/xx « Gouvernance d'entreprise – banques » |
| Date : | … |
| Entrée en vigueur : | 1er juillet 2016 |
| Concordance : | remplace la Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » du 20 novembre 2008 |
| Bases légales : | LFINMA art. 7 al. 1 let. b<br>LB art. 3 al. 2 let. a, 3*b* à 3*g*, 4quinquies<br>OB art. 11 al. 2, 12<br>LBVM art. 10 al. 2 let. a et al. 5, 14<br>OBVM art. 19, 20<br>OFR art. 7 à 12 |
| Annexe : | n. a. |

| **Destinataires** | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LB | | | LSA | | | LBVM | | LPCC | | | | | | | | LBA | | | Autres | |
| Banques | Groupes et congl. financiers | Autres intermédiaires | Assureurs | Groupes et congl. d'assur. | Intermédiaires d'assur. | Bourses et participants | Négociants en valeurs mob. | Directions de fonds | SICAV | Sociétés en comm. de PCC | SICAF | Banques dépositaires | Gestionnaires de PCC | Distributeurs | Représentants de PCC étr. | Autres intermédiaires | OAR | IFDS | Entités surveillées par OAR | Sociétés d'audit | Agences de notation |
| x | x | | | | | | x | | | | | | | | | | | | | | |

Laupenstrasse 27, 3003 Berne
Tél. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
**www.finma.ch**

# Table des matières

# Table des matières

*Explication de l'arrière-plan de couleur*

Vient de la Circ.-FINMA 08/24 (avec adaptations de la formulation)

Vient des Circ.-FINMA 08/21 et 08/32 (avec adaptations de la formulation)

Directives internationales (notamment les « Principes de gouvernance d'entreprise à l'intention des banques » du CBCB)

FAQ sur la direction supérieure

## I. Objet

La présente circulaire explique les exigences à l'égard de la gouvernance d'entreprise, au système de contrôle interne et à la gestion des risques chez les banques, les négociants en valeurs mobilières, les groupes financiers (art. 3*c* al. 1 LB) et les conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières (art. 3*c* al. 2 LB). Ceux-ci sont désignés ci-après par le terme d'« établissements ». 1

La gouvernance d'entreprise désigne ci-après les principes et les structures sur la base desquels un établissement est conduit et contrôlé par ses organes. La gouvernance d'entreprise a pour but de réaliser un équilibre fonctionnel entre les divers organes de l'entreprise *(« checks and balances »),* une transparence suffisante des processus internes de l'entreprise ainsi que l'harmonisation des objectifs de l'entreprise avec les attentes des divers groupes d'ayants droit. 2

## II. Définitions

La gestion des risques englobe les structures organisationnelles ainsi que les méthodes et les processus qui servent à la définition des stratégies de risque et des mesures de pilotage en matière de risques, mais aussi à l'identification, à la mesure, à l'administration, à la surveillance et à l'établissement de rapports sur les risques. 3

Le contrôle des risques surveille, en tant qu'instance de contrôle indépendante, le profil de risque de l'établissement et fournit les informations nécessaires à la surveillance des risques. 4

L'appétence au risque inclut des considérations tant quantitatives que qualitatives concernant les principaux risques que l'établissement est prêt à assumer pour atteindre ses objectifs commerciaux stratégiques, compte tenu de sa planification des fonds propres et des liquidités. L'appétence au risque est fixée pour chaque catégorie de risques, mais aussi au niveau de l'établissement. 5

Le profil de risque correspond à chaque position de risques de l'établissement prise au niveau de l'établissement et pour chacune des catégories de risques à un moment donné. 6

Le système de contrôle interne comporte les processus, les méthodes et les mesures définis au sein de l'établissement et qui servent à garantir une sécurité adéquate concernant l'efficacité des processus d'activité, la fiabilité du rapport financier, la réduction des risques et le respect des lois et des prescriptions. 7

La fonction de *compliance* contrôle la conformité aux prescriptions réglementaires et internes ainsi que le respect des normes et règles déontologiques en usage sur le marché. 8

## III. Champ d'application (principe de proportionnalité)

La présente circulaire s'applique à tous les établissements selon le Cm 1. Les exigences doivent être concrétisées au cas par cas, en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement. Les chiffres marginaux indiquent quand des établissements des catégories de surveillance 4 et 5 sont exemptés de façon générale de l'application. La FINMA peut ordonner des allègements ou des renforcements au cas par cas. 9

## IV. Organe responsable de la direction supérieure

### A. Tâches et responsabilités

L'organe exerçant la haute direction, la surveillance et le contrôle élabore les objectifs stratégiques, définit les moyens nécessaires pour atteindre ces objectifs et contrôle la direction dans la perspective de la poursuite desdits objectifs. 10

Ses tâches sont notamment les suivantes : 11

**a) Stratégie commerciale et politique de risque**

Sur proposition de la direction, l'organe responsable de la direction supérieure détermine la stratégie commerciale, fixe les principaux objectifs de l'entreprise ainsi que la charte de l'entreprise et édicte des principes directeurs concernant la culture d'entreprise et les valeurs de l'entreprise. Elle approuve le concept-cadre pour la gestion des risques à l'échelle de l'établissement et supporte la responsabilité de la réglementation, de la mise en place et de la surveillance d'une gestion des risques efficace ainsi que du pilotage des risques globaux. Elle appréhende les structures de l'entreprise et les risques de chaque champ d'activité de l'établissement. 12

### b) Organisation

L'organe responsable de la direction supérieure est responsable d'une organisation appropriée de l'entreprise et de l'équilibre des *« checks and balances »*. Il édicte les règlements, notamment les règlements d'organisation et opérationnel, et les directives nécessaires à l'exploitation commerciale, à la répartition des compétences et à la surveillance. 13

### c) Finances

L'organe responsable de la direction supérieure porte la responsabilité suprême pour la situation financière et le développement de l'établissement. Il veille à un aménagement efficace de la comptabilité et du contrôle des finances, et approuve périodiquement la planification des fonds propres et des liquidités établie par la direction. Il est chargé de l'adoption du rapport de gestion, du budget annuel, des comptes intermédiaires ainsi que des objectifs financiers annuels. 14

### d) Ressources humaines et autres ressources

L'organe responsable de la direction supérieure doit garantir que l'établissement dispose de ressources appropriées, tant humaines qu'autres (par ex. infrastructure, informatique). Il adopte la politique en matière de personnel et de rémunération et décide de la nomination et de la révocation des membres de son comité, des membres de la direction, du président de celle-ci ainsi que des autres personnes à la tête des fonctions de contrôle et des fonctions-clés (par ex. Chief Risk Officer, Chief Compliance Officer, Head IT). 15

### e) Surveillance et contrôle

L'organe responsable de la direction supérieure exerce la haute surveillance sur la direction et garantit la *compliance* au sein de l'établissement. Il veille au caractère approprié de l'environnement de contrôle et de risque au sein de l'établissement. Il met en place un système de contrôle interne efficace, mandate et surveille la révision interne, désigne la société d'audit prudentielle et en évalue les rapports. L'organe responsable de la direction supérieure ou son 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

### f) Changements structurels et investissements

L'organe responsable de la direction supérieure statue sur les points suivants : changements apportés à la structure de l'entreprise, créations et fermetures de succursales et filiales significatives, acquisitions et aliénations significatives, fusions, externalisations d'activités, changements essentiels touchant des filiales significatives et autres projets d'importance stratégique. 17

## B. Membres de l'organe responsable de la direction supérieure

### a) Conditions générales

Les membres de l'organe responsable de la direction supérieure doivent jouir d'une bonne réputation et offrir la garantie d'une activité irréprochable. Ils sont intègres et disposent, en tant qu'organe collectif, des compétences de gestion suffisantes ainsi que des connaissances techniques et de l'expérience nécessaires dans les secteurs bancaire et financier. L'organe responsable de la direction supérieure doit être composé de manière suffisamment diversifiée afin que, outre les principaux champs d'activité, tous les autres domaines centraux que sont la finance et la comptabilité, la gestion des risques, le *controlling*, la *compliance* et l'informatique soient représentés avec les compétences requises. Chaque membre dispose d'au moins une connaissance approfondie qui contribue à l'équilibre de l'organe collectif. 18

Dans son ensemble et selon l'orientation géographique de l'activité, l'organe responsable de la direction supérieure doit être suffisamment familier avec les marchés locaux, régionaux, nationaux et internationaux ainsi qu'avec le cadre réglementaire correspondant. 19

### b) Indépendance

Les membres de l'organe responsable de la direction supérieure organisent leurs rapports personnels et professionnels de manière à éviter autant que possible les conflits d'intérêts avec l'établissement. Ils ne font pas simultanément partie de la direction opérationnelle. Ils n'exercent en principe aucune activité opérationnelle pour l'établissement. 20

L'organe responsable de la direction supérieure dispose d'un nombre suffisant de membres indépendants qui n'ont aucune proximité particulière avec l'établissement. Il est composé pour un tiers au moins de membres indépendants. La FINMA peut autoriser des exceptions s'il existe de justes motifs. 21

Un membre de l'organe responsable de la direction supérieure est réputé indépendant s'il satisfait au moins aux critères suivants : 22

- il n'occupe pas d'autre fonction dans l'établissement et n'en a pas occupé au cours des deux dernières années ; 23
- 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 ; et 24
- il n'entretient avec l'établissement aucune relation d'affaires qui, par sa nature ou son ampleur, conduit à un conflit d'intérêts. 25

Une partie déterminante de l'organe responsable de la direction supérieure ne doit par ailleurs pas détenir de participation qualifiée dans l'établissement ou ne doit pas 26

représenter un détenteur d'une participation qualifiée. Les intérêts des créanciers au niveau de l'établissement individuel priment les intérêts des groupes et des propriétaires, notamment si ceux-ci en diffèrent.

Les membres de l'organe responsable de la direction supérieure 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 si : 27

- 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 28

- ils ne reçoivent pas d'instructions de l'organe qui les a élus relatives à leur activité en tant que membres de l'organe responsable de la direction supérieure. 29

## C. Principes de la gestion du mandat

Chaque membre de l'organe responsable de la direction supérieure doit consacrer le temps suffisant à l'exercice de son mandat et participer activement à la conduite stratégique de l'entreprise. Il doit exercer son mandat en personne et se tenir prêt à assumer durablement un rythme de réunions supérieur à la normale en cas de situations de crise ou d'urgence. Il convient d'accorder le nombre et le type d'autres mandats et activités exercés avec les exigences concrètes inhérentes au mandat à la direction supérieure de façon à ce que celui-ci puisse être exercé avec le soin requis. 30

L'organe responsable de la direction supérieure détermine le profil d'exigences posé a ses membres, à son président et aux membres éventuels de ses comités ainsi qu'au président de la direction. Il approuve et évalue périodiquement le profil demandé aux autres membres de la direction ainsi qu'aux personnes-clés. Il assure la planification de la relève. 31

L'organe responsable de la direction supérieure évalue au moins une fois par an, éventuellement en recourant aux services d'un tiers, ses propres performances (réalisation des objectifs et mode de travail) de manière critique et en consigne les résultats par écrit. Ses membres continuent de se former de manière ciblée et sont toujours au fait des dernières évolutions ayant lieu dans les principaux secteurs importants pour l'activité de l'entreprise, y compris ceux touchant l'environnement réglementaire. Les nouveaux élus sont introduits à leurs tâches et obligations. 32

L'organe responsable de la direction supérieure règle le traitement des conflits d'intérêts et détermine les conditions et modalités de récusation. Les intérêts existants et passés doivent être déclarés et les conflits d'intérêts, efficacement réglés. Le membre doit remettre son mandat si un conflit d'intérêt ne peut pas être durablement évité. 33

## D. Partage des tâches et comités

### a) Rôle du président

Le président est une personne présentant une faculté de jugement, des capacités de gestion et une intégrité exceptionnelles. Il marque de façon décisive la stratégie, la communication et la culture de l'entreprise. 34

Il est à la tête de l'organe collectif et est responsable de son bon fonctionnement conformément au règlement. Il représente l'organe responsable de la direction supérieure tant à l'intérieur de l'entreprise que vis-à-vis de l'extérieur. Il entretient un dialogue régulier avec le président de la direction et les autres membres de celle-ci, avec les personnes à la tête des fonctions de contrôle et est responsable de la préparation et de la diffusion du flux d'informations au sein de l'organe responsable de la direction supérieure. 35

### b) Comités

L'organe responsable de la direction supérieure peut instaurer en son sein des comités chargés de le seconder ou confier des tâches à certains de ses membres. Les établissements des catégories de surveillance 1 à 3 doivent instituer un comité d'audit et un comité des risques séparés. Les banques d'importance systémique doivent disposer de comités supplémentaires et impérativement d'un comité des rémunérations et des nominations qui assiste l'organe responsable de la direction supérieure lors de la définition de la politique en matière de rémunération, de l'élaboration des principes de sélection des cadres dirigeants, de la préparation et de l'exécution des décisions relatives au personnel ainsi que de la planification de la relève et qui surveille par ailleurs la mise en œuvre de la politique en matière de rémunération. Les comités assurent un *reporting* approprié à l'organe responsable de la direction supérieure dans son ensemble. 36

De par sa composition, le comité d'audit doit suffisamment se démarquer des autres comités. 37

La majorité des membres du comité d'audit, du comité des risques et du comité des nominations doivent en principe être indépendants (cf. Cm 20 ss). La FINMA peut accorder des allègements aux groupes financiers. En principe, le président de l'organe responsable de la direction supérieure ne devrait ni faire partie du comité d'audit ni présider un autre comité. Les membres de tous les comités doivent, globalement, disposer d'excellentes connaissances et d'une expérience suffisante dans le domaine d'activité du comité où ils siègent. 38

Les tâches et le fonctionnement des comités permanents doivent être fixés par l'organe responsable de la direction supérieure dans un règlement d'organisation. 39

### c) Tâches du comité d'audit

Ses tâches sont notamment les suivantes : 40

- élaboration de directives générales concernant la révision interne et le rapport financier à l'intention de l'ensemble de l'organe responsable de la direction supérieure ; 41
- surveillance et évaluation du rapport financier et de l'intégrité des bouclements financiers, y compris leur discussion avec le membre de la direction chargé des finances et de la comptabilité, le réviseur responsable ainsi que le responsable de la révision interne ; 42
- surveillance et évaluation de l'efficacité des contrôles internes, notamment aussi du contrôle des risques et de la fonction de *compliance* ainsi que de la révision interne ; 43
- surveillance et évaluation de l'efficacité et de l'indépendance de la société d'audit ainsi que de sa collaboration avec la révision interne, y compris la discussion des rapports d'audit avec l'auditeur responsable ; 44
- examen du plan d'audit, du rythme d'audit et des résultats d'audit de la révision interne et de la société d'audit. 45

### d) Tâches du comité des risques

Ses tâches sont notamment les suivantes : 46

- discussion du concept-cadre pour la gestion des risques à l'échelle de l'établissement et soumission des recommandations correspondantes à l'ensemble de l'organe responsable de la direction supérieure ; 47
- examen de la planification des fonds propres et des liquidités et rapport correspondant à l'ensemble de l'organe responsable de la direction supérieure ;
- évaluation au moins annuelle du concept-cadre pour la gestion des risques à l'échelle de l'établissement et mise en œuvre des adaptations nécessaires ; 48
- vérification de l'entretien par l'établissement d'une gestion des risques appropriée avec des processus efficaces qui satisfont à la situation de l'établissement en matière de risques ; 49
- surveillance de la mise en œuvre des stratégies de risque, notamment dans la perspective de leur conformité avec l'appétence au risque prescrite et les limites posées en matière de risques selon le concept-cadre pour la gestion des risques à l'échelle de l'établissement. 50

Le comité des risques reçoit régulièrement du Chief Risk Officer (CRO) et d'autres titulaires 51

de fonctions pertinents des rapports explicites sur les différents aspects du concept-cadre pour la gestion des risques à l'échelle de l'établissement (selon les Cm 66 ss) et leur respect.

Des flux d'informations appropriés doivent être mis en place entre le comité d'audit et le comité des risques afin de permettre une coordination mutuelle efficace et une réaction appropriée aux modifications du profil de risque de l'établissement. 52

## V. Direction

### A. Tâches et responsabilités

La direction est responsable de l'activité opérationnelle en conformité avec la stratégie commerciale, le concept-cadre pour la gestion des risques à l'échelle de l'établissement et les autres principes, règles commerciales et d'organisation adoptés par l'organe responsable de la direction supérieure. Elle exécute les décisions de l'organe responsable de la direction supérieure et est responsable du respect des prescriptions prudentielles dans le cadre de l'activité opérationnelle. 53

La direction est notamment responsable : 54

- de la conduite des affaires courantes et de la représentation de l'établissement vis-à-vis des tiers dans le secteur opérationnel ; 55
- de la formulation de propositions concernant les affaires qui relèvent de la compétence ou nécessitent l'approbation de l'organe responsable de la direction supérieure, notamment l'élaboration de la politique commerciale, du concept-cadre pour la gestion des risques à l'échelle de l'établissement, de la charte et des objectifs de l'entreprise ; 56
- d'une structure de conduite et d'organisation à l'échelle de l'établissement qui assure les responsabilités, compétences, obligations de rendre compte, pouvoirs d'injonction et de décision ainsi qu'une séparation appropriée des fonctions ; 57
- de l'entretien d'un système d'information du management (MIS), sachant que les flux d'informations doivent être définis afin de collecter et de traiter toutes les informations importantes sur l'évolution de l'entreprise et de les mettre à la disposition de l'organe responsable de la direction supérieure sous une forme appropriée ; 58
- de la conception et de l'entretien d'un système de contrôle interne (SCI) selon le Cm 79 ; 59
- du pilotage opérationnel des revenus et des risques, y compris la gestion de la structure du bilan ; 60
- de l'édiction de prescriptions visant à régler l'exploitation commerciale opérationnelle ; 61

- d'une infrastructure technologique adéquate dont les capacités tiennent suffisamment compte des besoins commerciaux actuels et à plus long terme et permettent d'atténuer les risques opérationnels, de répondre aux exigences de l'exploitation ordinaire et des phases de crise et de garantir la sécurité, l'intégrité et la disponibilité des données et systèmes ; 62

- de la conformité aux prescriptions prudentielles et aux directives internes des adaptations prévues de l'activité commerciale, qui se caractérisent notamment par la constitution de sociétés ou de succursales suisses et étrangères ou la participation dans celles-ci ou par l'introduction de nouveaux services, de produits et de solutions financiers. 63

### B. Exigences à l'égard des membres de la direction

Les membres de la direction doivent jouir d'une bonne réputation et offrir la garantie d'une activité irréprochable. Ils sont intègres et disposent, en tant qu'organe collectif et en tant que responsables de fonctions, des compétences de gestion suffisantes ainsi que des connaissances techniques et de l'expérience nécessaires dans les secteurs bancaire et financier pour assurer l'activité opérationnelle de manière appropriée. Par leur comportement personnel, les membres de la direction contribuent à la culture d'entreprise et de risque. 64

Dans son ensemble et selon l'orientation géographique de l'activité, la direction doit être suffisamment familière avec les marchés locaux, régionaux, nationaux et internationaux et le cadre réglementaire correspondant. 65

## VI. Concept-cadre pour la gestion des risques à l'échelle de l'établissement

Le concept-cadre pour la gestion des risques à l'échelle de l'établissement est élaboré par la direction et adopté par l'organe responsable de la direction supérieure. 66

Il définit la politique de risque, l'appétence au risque ainsi que les limites posées en matière de risques et consigne la nature, le type et le niveau des risques auxquels est exposé l'établissement et qu'il est prêt à prendre. 67

Le concept-cadre doit au moins intégrer les aspects suivants : 68

- catégorisation uniforme des risques principaux afin d'assurer la cohérence des objectifs au niveau de la gestion des risques, de leur identification, de leur mesure, de leur administration, de leur surveillance et de l'établissement de rapports sur les risques ; 69

- précision des risques spécifiques à l'établissement et de la perte pouvant en résulter, en référence aux définitions prudentielles et détermination et utilisation des instruments d'identification, de mesure, d'administration et de surveillance de toutes les catégories 70

de risques ;

- définition de l'appétence au risque et des limites posées en matière de risques par rapport à l'ensemble des catégories de risques et définition des stratégies et instruments d'atténuation des risques ; 71

- définition des mesures permettant d'identifier à temps les violations des limites posées en matière de risques et d'y remédier ; 72

- mise en place de structures organisationnelles pour l'administration de toutes les catégories de risques, y compris les compétences, les obligations de rendre compte et les lignes de *reporting* ; 73

- conception d'une documentation permettant une compréhension indépendante appropriée ainsi qu'une évaluation et une vérification de la définition de l'appétence au risque et des limites posées en matière de risques ; 74

- entretien d'un système de production de rapports sur les risques et d'information du management (MIS) pour toutes les catégories de risques ; 75

- obligation de vérifier et d'adapter éventuellement le concept-cadre dans les meilleurs délais et en permanence en cas de modification essentielle de la situation de risque par une unité d'organisation clairement désignée, dotée d'un personnel qualifié suffisant ; 76

- prescriptions concernant une application cohérente du concept-cadre à l'échelle de l'établissement, notamment en ce qui concerne tous les produits, activités, processus et systèmes nouveaux et actuels importants ; 77

- dispositions relatives à l'agrégation des risques et aux rapports sur les risques dans les banques d'importance systémique. 78

## VII. Système de contrôle interne

L'établissement doit disposer d'un système de contrôle interne documenté adéquat qui se compose de règles, processus et systèmes. Il doit notamment inclure l'identification, la mesure, l'administration et la surveillance des risques encourus par l'établissement en tant que partie intégrante de l'ensemble des processus de travail. Des contrôles doivent par ailleurs être prévus afin d'identifier à temps notamment les violations des limites posées en matière de risques et les écarts par rapport à la politique de risque fixée. Dans ce cadre, l'établissement financier doit mettre en place des stratégies appropriées de transfert et/ou d'atténuation des risques. 79

Les instances de contrôle englobent au moins trois domaines différents de l'établissement : les unités d'affaires génératrices de revenus, les instances de contrôle indépendantes des unités d'affaires génératrices de revenus et la révision interne. 80

## A. Unités d'affaires génératrices de revenus

Les unités d'affaires génératrices de revenus assument leur fonction de contrôle dans le cadre des affaires courantes en gérant les risques et plus particulièrement en en assurant la surveillance directe, le pilotage et le *reporting*. 81

## B. Instances de contrôle indépendantes

Le système de rémunération des instances de contrôle indépendantes ne doit pas comprendre d'éléments susceptibles de générer des conflits d'intérêts avec leurs tâches. Le calcul de la rémunération variable de ces personnes ne doit pas dépendre directement du résultat des unités d'affaires à surveiller, de produits ou de transactions spécifiques. 82

### a) Instauration et positionnement hiérarchique

Les instances de contrôle indépendantes disposent d'un droit illimité à l'information, à son accès et à sa consultation dans le cadre de leurs tâches et doivent être intégrées dans l'organisation globale de l'établissement et le système de contrôle interne, indépendamment des unités d'affaires génératrices de revenus. 83

Les instances de contrôle indépendantes doivent être dotées de ressources et de compétences appropriées. Chaque établissement doit garantir une évaluation des unités d'affaires génératrices de revenus efficace et orientée sur les risques, fondée sur l'expérience et la qualification des collaborateurs. Les collaborateurs des instances de contrôle indépendantes doivent suivre des formations et des perfectionnements réguliers à ce sujet. 84

L'établissement confie la responsabilité des instances de contrôle indépendante à un ou plusieurs membres de la direction. 85

L'établissement s'assure que les instances de contrôle indépendantes disposent d'un accès direct et régulier à l'organe responsable de la direction supérieure ou à son comité des risques. 86

Les établissements des catégories de surveillance 1 à 3 disposent d'un contrôle des risques et d'une fonction de *compliance* autonomes l'un de l'autre en tant qu'instances de contrôles indépendantes. Ils désignent un CRO responsable du contrôle des risques. 87

Les banques d'importance systémique désignent un CRO qui est membre de la direction et qui est exclusivement chargé du contrôle des risques. 88

### b) Tâches et responsabilités du contrôle des risques

Le contrôle des risques assure le caractère systématique et exhaustif de la surveillance et de l'établissement de rapports sur des positions-risque individuelles ou agrégées. En tant 89

que composante des analyses quantitatives et qualitatives, cela implique la réalisation de tests de résistance et d'analyses de scénarios dans des conditions commerciales défavorables.

Le contrôle des risques surveille le profil de risque de l'établissement, notamment à l'aune de l'appétence au risque et des limites posées en matière de risques définis dans le concept-cadre pour la gestion des risques à l'échelle de l'établissement. 90

Il fournit les informations nécessaires à la surveillance des risques. 91

Il incombe en outre au contrôle des risques d'élaborer et de mettre en place des systèmes de surveillance des risques adéquats et de les adapter en fonction des nouvelles activités commerciales et des nouveaux produits et services financiers, 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 utilisés pour le respect des prescriptions prudentielles (notamment les dispositions en matière de fonds propres, de répartition des risques et de liquidités). 92

Le contrôle des risques participe au processus de développement des produits, services, domaines d'activité ou secteurs de marché nouveaux ou étendus ou des transactions complexes et à l'examen de la diligence *(due diligence)*. 93

Il informe la direction des principales hypothèses et des lacunes des modèles et analyses de risques, sous une forme appropriée. 94

Le contrôle des risques garantit par ailleurs que les limites posées en matière de risques sont notamment en conformité avec l'appétence au risque et avec les résultats des tests de résistance et qu'elles ont été définies de manière à constituer un instrument de pilotage efficace au plan opérationnel. Le contrôle des risques s'assure en outre de l'existence de procédures claires et documentées concernant la gestion des autorisations pour la fixation et la modification des limites et en cas d'infractions. 95

Dans le cas des banques d'importance systémique, le contrôle des risques vérifie la mise en œuvre appropriée des dispositions relatives à l'agrégation des données de risque et au rapport sur les risques, qui font partie intégrante du concept-cadre pour la gestion des risques à l'échelle de l'établissement approuvé par l'organe responsable de la direction supérieure. Le contrôle des risques s'assure notamment que l'établissement dispose d'une architecture des données et d'une infrastructure informatique autorisant une mesure rapide et agrégée des risques, une agrégation des données de risque et un rapport sur les risques pour toutes les catégories de risques importantes de l'établissement, tant dans des conditions normales que dans des périodes de crise. Le contrôle des risques vérifie par ailleurs qu'il existe des ressources appropriées à cet effet. 96

Le contrôle des risques remet au moins une fois par semestre un rapport à la direction relatif aux risques et aux positions-risque. En cas d'évolution particulière de la situation, il en informe immédiatement la direction et la révision interne et, en cas de faits de grande 97

portée, l'organe responsable de la direction supérieure et le comité des risques.

Au moins une fois par année, le contrôle des risques présente à l'organe responsable de la direction supérieure un rapport sur l'évolution du profil de risque de l'établissement et sur son activité telle que définie aux Cm 89 ss. Le contrôle des risques informe par ailleurs immédiatement l'organe responsable de la direction supérieure des violations des limites posées en matière de risques autorisées par ce dernier. Une copie de ces rapports doit aussi être mise à disposition de la révision interne et de la société d'audit. 98

**c) Tâches et responsabilités de la fonction de *compliance***

En règle générale, les tâches et les responsabilités de la fonction de *compliance* en tant qu'instance de contrôle indépendante comprennent les activités suivantes : 99

- 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. Le plan d'action doit aussi être mis à disposition de la révision interne ; 100

- 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 lors du choix des instructions à donner ou des mesures à prendre. La révision interne doit en être informée ; 101

- la remise à l'organe responsable de la direction supérieure d'un rapport annuel sur l'évaluation du risque de *compliance* et l'activité de la fonction de *compliance*. Une copie du rapport doit être mise à disposition de la révision interne et aussi de la société d'audit. 102

En plus de ses tâches et responsabilités dans son rôle d'instance de contrôle indépendante, la fonction de *compliance* soutient et conseille la direction ainsi que les collaborateurs lors de l'élaboration, de l'application et de la surveillance des prescriptions réglementaires et internes et soutient la direction dans la formation et l'information des collaborateurs en matière de *compliance*. 103

## VIII. Révision interne

### A. Instauration

Chaque établissement est tenu d'instaurer une révision interne. 104

Dans des cas particuliers, la FINMA peut, après consultation de la société d'audit, exempter un établissement de l'obligation prévue au Cm 104. 105

Lorsque l'instauration d'une révision interne propre à l'établissement n'apparaît pas appropriée, les tâches de révision interne peuvent être confiées à : 106

- 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), 107

- une seconde société d'audit indépendante de celle de l'établissement, ou 108

- un tiers indépendant, à condition que la société d'audit confirme ses compétences professionnelles et ses ressources techniques et personnelles appropriées. 109

## B. Positionnement hiérarchique et organisation

La révision interne est subordonnée à l'organe responsable de la direction supérieure ou à son comité d'audit et elle exécute les tâches de révision et de surveillance qui lui sont confiées en toute indépendance. 110

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 et indépendante de l'exploitation commerciale. Elle doit disposer d'un personnel suffisant et réunir les connaissances techniques nécessaires pour exécuter son mandat. 111

Le responsable de la révision interne est nommé par l'organe responsable de la direction supérieure. 112

La révision interne travaille indépendamment des processus d'affaires quotidiens et elle dispose d'un droit d'accès et de contrôle illimité au sein de l'établissement et de ses entreprises devant être consolidées au sens du Cm 125. Tous les renseignements nécessaires à l'accomplissement de ses travaux d'audit doivent être mis à sa disposition. 113

Les bases nécessaires à la révision interne, telles qu'un règlement précisant son organisation, ses tâches et ses responsabilités, doivent être édictées par l'organe responsable de la direction supérieure ou son comité d'audit. Pour le reste, la révision interne définit elle-même son mode de travail (par exemple méthodologie, types d'audits, formations et perfectionnements). 114

La révision interne doit répondre aux exigences qualitatives de l'Association suisse d'audit interne (ASAI). Le travail de la révision interne est fondé sur les *Standards for the Professional Practice* de l'Institute of Internal Auditors (IIA). 115

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 116

succès de produits ou transactions spécifiques.

## C. Tâches et responsabilités

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. 117

Elle 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, orientation de l'activité). 118

Sur la base de cette évaluation des risques, la révision interne fixe les objectifs d'audit et la planification de l'audit de la période d'audit suivante et demande leur approbation par l'organe responsable de la direction supérieure ou son comité d'audit. Si des modifications importantes du profil de risque surviennent durant la période d'audit, la révision interne adapte les objectifs d'audit et la planification de l'audit et en demande de nouveau l'approbation. 119

La révision interne s'assure que la direction soit informée de l'évaluation des risques et des objectifs d'audit et que la société d'audit reçoive une copie de ces documents. 120

En outre, elle 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. 121

La révision interne rend compte à l'organe responsable de la direction supérieure ou à son comité d'audit et à la direction, en temps utile et par écrit, de toutes les constatations importantes effectuées dans le cadre d'un audit. 122

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, à l'organe responsable de la direction supérieure ou à son comité d'audit pour information. Ce rapport sera également adressé à la direction et à la société d'audit. 123

En outre, la révision interne informe au moins une fois par semestre l'organe responsable de la direction supérieure ou son comité d'audit 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 aussi être assurés par une autre instance indépendante au sein de l'établissement, par exemple par la fonction de *compliance* ou le contrôle des risques. 124

## IX. Structures de groupe

Les principes et dispositions de cette circulaire s'appliquent par analogie aux groupes et conglomérats financiers (« groupes »). 125

Les groupes doivent régler les tâches et les responsabilités selon la présente circulaire au niveau de l'organe responsable de la direction supérieure et de la direction des unités ayant une responsabilité globale pour la conduite du groupe. Il faut s'assurer qu'il existe des prescriptions qui tiennent suffisamment compte des structures juridiques et organisationnelles, des tâches et des responsabilités ainsi que de l'indépendance des niveaux de conduite respectifs, de l'activité commerciale et des principaux risques au niveau du groupe et de l'établissement individuel. Il convient en particulier de prendre en compte les risques résultant du regroupement de plusieurs entreprises en une entité économique unique. 126

La révision interne du groupe s'étend au minimum à toutes les entreprises devant être consolidées. 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. 127

## X. Publication

Les principes et les structures grâce auxquels un établissement est piloté et contrôlé ainsi que la gestion des risques doivent être présentés en toute transparence aux déposants, investisseurs, acteurs du marché et autres groupes d'ayants droit. 128

Les informations suivantes doivent être rendues publiques : 129

- La composition de l'organe responsable de la direction supérieure ainsi que le parcours professionnel et la formation de ses différents membres. Les membres indépendants selon les Cm 21 ss doivent être indiqués. 130
- L'organisation de l'organe responsable de la direction supérieure, notamment la présidence ainsi que la constitution éventuelle et la composition des comités selon les Cm 36 ss. 131
- La composition de la direction ainsi que le parcours professionnel et la formation de ses différents membres. 132
- Les principes de la procédure d'élection des membres de l'organe responsable de la direction supérieure et le processus de recrutement des membres de la direction. 133
- L'orientation stratégique en matière de risques et le profil de risque de l'établissement ainsi que l'évaluation de la situation en matière de risque par la direction. 134

Les informations suivantes de la directive de SIX Exchange concernant les informations relatives à la *corporate governance* doivent être publiées par les établissements des catégories de surveillance 1 à 3 : 135

- La structure du groupe (groupe financier) ainsi que les actionnaires importants et les participations croisées éventuelles. (ch 1. de la directive de SIX) 136
- Les autres activités et groupements d'intérêt des membres de l'organe responsable de la direction supérieure. (ch. 3.2) 137
- L'organisation interne et la méthode de travail de l'organe responsable de la direction supérieure ainsi que les instruments d'information et de contrôle à l'égard de la direction. (ch. 3.5 à 3.7) 138
- Les autres activités et groupements d'intérêt des membres de la direction. (ch. 4.2) 139
- Les bases et les éléments des rémunérations et des programmes de participation pour les membres de l'organe responsable de la direction supérieure et de la direction ainsi que la compétence et la procédure pour leur fixation. (ch. 5.1) 140
- Concernant l'organe de révision et la société d'audit prudentielle, la durée du mandat de révision et d'audit, la durée de la fonction du réviseur responsable et de l'auditeur responsable, les honoraires de révision et d'audit pour l'exercice écoulé, les honoraires supplémentaires ainsi que les instruments d'information de la société de révision vis-à-vis de l'organe responsable de la direction supérieure. (ch. 8.1 à 8.4) 141
- La politique d'information appliquée par l'établissement. (ch. 9) 142

La publication s'effectue de manière facilement accessible sur le site Internet de l'établissement et dans un chapitre séparé du rapport de gestion. Les changements matériels sont mis à jour sur le site Internet dans un délai d'un mois. Il est possible de renoncer à une publication séparée si certaines informations sont déjà publiées dans le rapport de gestion ordinaire ou sur la base des exigences de la Circ.-FINMA 16/1 « Publication – banques ». 143

## XI. Entrée en vigueur et dispositions transitoires

La présente circulaire entre en vigueur le […]. 144

Les exigences suivantes devront être concrétisées au plus tard un an après l'entrée en vigueur : 145

La mise en œuvre de la règle du tiers concernant l'indépendance de l'organe responsable de la direction supérieure selon le Cm 21.

L'introduction d'un comité d'audit et d'un comité des risques séparé pour les

établissements des catégories de surveillance 1 à 3 selon les Cm 36 ss et les Cm 46 ss.

L'élaboration et l'approbation d'un concept-cadre pour la gestion des risques à l'échelle de l'établissement selon le Cm 66.

La mise en place d'un poste de CRO séparé, notamment dans le cadre de la direction pour les banques d'importance systémique selon les Cm 87 et 88.

La FINMA peut prolonger le délai transitoire dans des cas particuliers justifiés.