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 2017/1
Gouvernance d'entreprise – banques

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

Référence :	Circ.-FINMA 17/1 « Gouvernance d'entreprise – banques »
Date :	22 septembre 2016
Entrée en vigueur :	1er juillet 2017
Dernière modification :	4 novembre 2020 [les modifications sont signalées par * et figurent à la fin du document]
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 LB art. 3 al. 2 let. a et c, 3*b* à 3*f*, 4quinquies, 6 OB art. 11 al. 2, 12 LEFin art. 7, 9, 49 OEFin art. 9, 12, 68 OFR art. 7 à 12

Destinataires

LB			LSA			LEFin						LIMF						LPCC						LBA		Autres	
Banques	Groupes et congl. financiers	Autres intermédiaires	Assureurs	Groupes et congl. d'assur.	Intermédiaires d'assur.	Gestionnaires de fortune	Trustees	Gestionnaires de fortune coll.	Directions de fonds	Maisons de titres tenant des comptes	Maisons de titres ne tenant pas de comptes	Plates-formes de négociation	Contreparties centrales	Dépositaires centraux	Référentiels centraux	Systèmes de paiement	Participants	SICAV	Sociétés en comm. de PCC	SICAF	Banques dépositaires	Représentants de PCC étr.	Autres intermédiaires	OAR	Entités surveillées par OAR	Sociétés d'audit	Agences de notation
X	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

I. Objet

La présente circulaire explique les exigences en matière de gouvernance d'entreprise, de gestion des risques, de système de contrôle interne (SCI) et de révision interne auprès des banques, des maisons de titres, des groupes financiers (art. 3*c* al. 1 LB) et des conglomérats financiers dominés par le secteur bancaire ou celui du négoce en valeurs mobilières (art. 3*c* al. 2 LB). Ceux-ci sont nommés ci-après « établissements ». 1

II. Définitions

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. 2

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, l'analyse, l'évaluation, la gestion, la surveillance des risques et à l'établissement de rapports sur les risques. 3

La tolérance 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. La tolérance au risque est fixée pour chaque catégorie de risques, mais aussi au niveau de l'établissement, pour autant que cela soit pertinent. 4

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. 5

Par système de contrôle interne (SCI), 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 de la réalisation des objectifs de la politique commerciale. Le SCI ne comprend pas uniquement les activités de contrôle a posteriori, mais également celles en rapport avec la gestion et la planification. Un SCI efficace englobe notamment des activités de contrôle intégrées dans les processus de travail, des processus de gestion des risques et de *compliance* appropriés, ainsi que des instances de contrôle adaptées à la taille, à la complexité et au profil de risque de l'établissement, notamment un contrôle des risques et une fonction de *compliance* indépendants. 6

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. 7

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 tenant compte de la taille, de la complexité, 8

de la structure et du profil de risque de l'établissement. La FINMA peut autoriser des allègements ou ordonner des renforcements au cas par cas.

IV. Organe responsable de la haute direction

A. Tâches et responsabilités

Les tâches de l'organe responsable de la haute direction, de la surveillance et du contrôle (ci-après « organe responsable de la haute direction ») sont notamment les suivantes : 9

a) Stratégie commerciale et politique de risque

L'organe responsable de la haute direction détermine la stratégie commerciale et édicte des principes directeurs concernant la culture d'entreprise. Il adopte la politique de risque ainsi que les principes de 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. 10*

b) Organisation

L'organe responsable de la haute direction est responsable d'une organisation appropriée de l'entreprise et édicte les règlements nécessaires à cet effet. 11

c) Finances

L'organe responsable de la haute direction porte la responsabilité suprême pour la situation financière et le développement de l'établissement. Il approuve et adopte la planification des fonds propres et des liquidités ainsi que le rapport de gestion, le budget annuel, les comptes intermédiaires et les objectifs financiers annuels. 12

d) Ressources humaines et autres ressources

L'organe responsable de la haute direction doit garantir que l'établissement dispose de ressources appropriées, tant humaines qu'autres (par ex. infrastructure, informatique) et assume la responsabilité de la politique en matière de personnel et de rémunération. Il 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 du *Chief Risk Officer* (CRO) et du responsable de la révision interne[1]. 13

e) Surveillance et contrôle

L'organe responsable de la haute direction exerce la haute surveillance sur la direction. Il est responsable du caractère approprié de l'environnement de contrôle et de risque au sein de l'établissement et veille à un SCI efficace. Il mandate et surveille la révision interne, désigne la société d'audit prudentielle et en évalue les rapports. 14

[1] Ce dernier peut également être choisi par le comité d'audit.

f) Changements structurels et investissements importants

L'organe responsable de la haute direction statue sur les points suivants : changements importants apportés à la structure de l'entreprise et du groupe, changements essentiels touchant des filiales significatives et autres projets d'importance stratégique. 15

B. Membres de l'organe responsable de la haute direction

a) Conditions générales

L'organe responsable de la haute direction dispose dans sa globalité des compétences de gestion suffisantes ainsi que des connaissances techniques et de l'expérience nécessaires dans les secteurs bancaire et financier. Il doit être composé de manière suffisamment diversifiée afin que, outre les principaux champs d'activité, tous les autres domaines centraux tels que la finance et la comptabilité ainsi que la gestion des risques soient représentés avec les compétences requises. 16

b) Indépendance

L'organe responsable de la haute direction est composé pour un tiers au moins de membres indépendants. La FINMA peut autoriser des exceptions s'il existe de justes motifs, par exemple pour les groupes financiers nationaux. 17

Un membre de l'organe responsable de la haute direction est réputé indépendant : 18

- s'il n'occupe pas d'autre fonction dans l'établissement et n'en a pas occupé au cours des deux dernières années ; 19
- s'il n'a pas occupé, au cours des deux dernières années, la fonction d'auditeur responsable de l'établissement au sein de la société d'audit ; 20
- s'il n'entretient avec l'établissement aucune relation d'affaires qui, par sa nature ou son ampleur, conduit à un conflit d'intérêts ; et 21
- s'il ne détient pas de participation qualifiée (au sens de l'art. 3 al. 2 let. c^{bis} LB et de l'art. 11 al. 4 LEFin) dans l'établissement, ni ne représente un détenteur d'une telle participation. 22

Les membres de l'organe responsable de la haute direction de banques cantonales ou communales désignés ou élus par les cantons, communes ou autres corporations de droit public cantonales ou communales sont réputés indépendants au sens des Cm 18 à 22 : 23

- s'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 24
- s'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 haute direction. 25

C. Principes de la gestion du mandat

Chaque membre de l'organe responsable de la haute direction 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. 26

L'organe responsable de la haute direction détermine le profil d'exigences posé à 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, au CRO et au responsable de la révision interne. Il assure la planification de la relève. 27

L'organe responsable de la haute direction 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. 28

L'organe responsable de la haute direction règle le traitement des conflits d'intérêts. Les intérêts existants et passés doivent être déclarés. L'établissement prend des mesures appropriées pour limiter efficacement ou éliminer un conflit d'intérêt inévitable. 29

D. Partage des tâches et comités

a) Rôle du président

Le président est à la tête de l'organe collectif et représente l'organe responsable de la haute direction tant à l'intérieur de l'entreprise que vis-à-vis de l'extérieur. Il marque de façon déterminante la stratégie, la communication et la culture de l'entreprise. 30

b) Comités

Les établissements des catégories de surveillance 1 à 3 doivent instituer un comité d'audit et un comité des risques. Les établissements de la catégorie de surveillance 3 peuvent également les réunir dans un comité mixte. Les établissements d'importance systémique doivent instituer au moins un comité des rémunérations et des nominations au niveau du groupe. Les comités assurent un *reporting* approprié à l'organe responsable de la haute direction dans son ensemble. 31

De par sa composition, le comité d'audit doit suffisamment se démarquer des autres comités. 32

La majorité des membres du comité d'audit et du comité des risques doivent en principe être indépendants (cf. Cm 18 à 25). En principe, le président de l'organe responsable de la haute direction ne devrait ni faire partie du comité d'audit ni présider le comité des risques. Les comités doivent, globalement, disposer de connaissances et d'une expérience suffisantes dans leur domaine d'activité. 33

c) Tâches du comité d'audit

Ses tâches sont notamment les suivantes : 34

- l'élaboration de directives générales concernant la révision interne et le rapport financier à l'intention de l'ensemble de l'organe responsable de la haute direction ; 35
- la surveillance et l'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 ; 36
- la surveillance et l'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, pour autant que cette tâche ne soit pas dévolue au comité des risques ; 37
- la 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 ; 38
- l'examen du plan d'audit, du rythme d'audit et des résultats d'audit de la révision interne et de la société d'audit. 39

d) Tâches du comité des risques

Ses tâches sont notamment les suivantes : 40

- la discussion de la politique de risque et des principes de la gestion des risques à l'échelle de l'établissement et la soumission des recommandations correspondantes à l'ensemble de l'organe responsable de la haute direction ; 41*
- l'examen de la planification des fonds propres et des liquidités ainsi que la remise du rapport correspondant à l'ensemble de l'organe responsable de la haute direction ; 42
- l'évaluation au moins annuelle de la politique de risque et des principes de la gestion des risques à l'échelle de l'établissement et la mise en œuvre des adaptations nécessaires ; 43*
- la 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 ; 44
- la surveillance de la mise en œuvre des stratégies de risque, notamment dans la perspective de leur conformité avec la tolérance au risque prescrite et les limites posées en matière de risques selon la politique de risque et les principes de la gestion des risques à l'échelle de l'établissement. 45*

Le comité des risques reçoit régulièrement du CRO et d'autres titulaires de fonctions pertinents des rapports explicites sur les différents aspects de la politique de risque et des principes de la gestion des risques à l'échelle de l'établissement (selon les Cm 52 à 59) et leur respect. 46*

V. Direction

A. Tâches et responsabilités

La direction est responsable de l'activité opérationnelle en conformité avec la stratégie commerciale, les prescriptions et les décisions de l'organe responsable de la haute direction et est notamment responsable : 47

- de la conduite des affaires courantes, du pilotage opérationnel des revenus et des risques, y compris la gestion de la structure du bilan et des liquidités, ainsi que de la représentation de l'établissement vis-à-vis des tiers dans le secteur opérationnel ; 48
- de la formulation de propositions concernant les affaires qui relèvent de la compétence ou nécessitent l'approbation de l'organe responsable de la haute direction et de l'édiction de prescriptions visant à régler l'exploitation commerciale opérationnelle ; 49
- de la conception et de l'entretien de processus internes adaptés, d'un système d'information du management approprié et d'un SCI ainsi que d'une infrastructure technologique adéquate. 50

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

Les membres de la direction disposent, en tant qu'organe collectif et en tant que responsables de différentes fonctions, des compétences de gestion suffisantes ainsi que des connaissances techniques et de l'expérience nécessaires dans les secteurs bancaire et financier pour assurer le respect des conditions d'octroi de l'autorisation dans le cadre de l'activité opérationnelle de manière appropriée. 51

VI. Politique de risque et principes de gestion des risques à l'échelle de l'établissement

La politique de risque et les principes de gestion des risques à l'échelle de l'établissement sont élaborés par la direction, adoptés par l'organe responsable de la haute direction et documentés sous une forme appropriée. 52*

La politique de risque et les principes de gestion des risques à l'échelle de l'établissement règlent la gestion des risques principaux, la tolérance au risque ainsi que les limites correspondantes en matière de risques dans toutes les catégories de risques importantes. 53*

Les établissements des catégories de surveillance 1 à 3 doivent notamment tenir compte des aspects suivants : 54*

- catégorisation uniforme[2] des risques principaux afin d'assurer la cohérence avec les objectifs au niveau de la gestion des risques ; 55

- précision de la perte pouvant résulter de ces catégories de risques importantes ; 56

- définition et utilisation des instruments ainsi que des structures organisationnelles d'identification, d'analyse, d'évaluation, de gestion, de surveillance des catégories de risques importantes et du *reporting* ; 57

- conception d'une documentation permettant une vérification appropriée de la définition de la tolérance au risque ainsi que des limites correspondantes posées en matière de risques ; 58

- dispositions relatives à l'agrégation des données de risque et aux rapports sur les risques dans les établissements des catégories de surveillance 1 à 3. Dans le cas des banques d'importance systémique, ces dispositions doivent notamment inclure des informations sur l'architecture des données et l'infrastructure informatique permettant une analyse et une évaluation rapides et agrégées des risques, ainsi qu'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. 59

VII. Système de contrôle interne

Il existe au moins deux instances de contrôle dans le cadre du SCI : les unités d'affaires génératrices de revenus et les instances de contrôle indépendantes à l'égard de celles-ci. 60

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*. 61

B. Instances de contrôle indépendantes

Les instances de contrôle indépendantes surveillent les risques ainsi que le respect des prescriptions légales, réglementaires et internes. Différentes instances de contrôle indépendantes peuvent être instituées selon les établissements, mais elles doivent au minimum assumer les tâches et les responsabilité du contrôle des risques (Cm 69 à 76) et de la fonction de *compliance* (Cm 77 à 81). 62

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. 63

[2] Par nature, type et niveau et en référence aux définitions prudentielles selon l'OFR.

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 SCI, de manière indépendante des unités d'affaires génératrices de revenus. Elles doivent être dotées de ressources et de compétences appropriées. 64

L'établissement confie la responsabilité des instances de contrôle indépendantes à un ou plusieurs membres de la direction. 65

Il s'assure que les instances de contrôle indépendantes disposent d'un accès direct à l'organe responsable de la haute direction. 66

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 qui, outre le contrôle des risques, peut aussi être responsable d'autres instances de contrôles indépendantes. 67

Les établissements d'importance systémique désignent un CRO qui est membre de la direction. 68

b) Tâches et responsabilités du contrôle des risques

Le contrôle des risques assure le caractère systématique de la surveillance et de l'établissement de rapports sur des positions-risque individuelles ou agrégées. En tant 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. Les établissements participant au régime des petites banques selon les art. 47*a* à 47*e* OFR doivent procéder au minimum à des analyses de scénarios. 69*

Dans les établissements des catégories de surveillance 1 à 3, le contrôle des risques assure en outre la mise en œuvre appropriée des dispositions relatives à l'agrégation des données de risque et aux rapports sur les risques selon le Cm 59. 70

Le contrôle des risques surveille le profil de risque de l'établissement, notamment à l'aune de la tolérance au risque et des limites posées en matière de risques définies par la politique de risque et les principes de gestion des risques à l'échelle de l'établissement. 71*

Il incombe en outre au contrôle des risques d'élaborer et d'exploiter des systèmes de surveillance des risques adéquats, de définir et d'appliquer des bases et des méthodes pour l'analyse et l'évaluation des risques (par ex. 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). 72

Le contrôle des risques est impliqué de manière appropriée dans le développement de 73

nouveaux types de produits, services, domaines d'activité ou secteurs de marché ou dans leur extension ainsi que dans les transactions importantes ou complexes.

Le contrôle des risques participe activement au processus de définition des limites posées en matière de risques et s'assure qu'elles sont notamment en conformité avec la tolérance 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 pour la direction. 74

Le contrôle des risques remet un rapport sur l'évolution du profil de risque de l'établissement et son activité selon les Cm 69 à 78 à la direction, au moins une fois par semestre, et à l'organe responsable de la haute direction, au moins une fois par an. Une copie de ces rapports doit être aussi mise à disposition de la révision interne et de la société d'audit. 75

En cas d'évolution particulière de la situation, le contrôle des risques en informe la direction et la révision interne en temps utile et, en cas de faits de grande portée, l'organe responsable de la haute direction. 76

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

Les tâches et les responsabilités de la fonction de *compliance* comprennent au moins les activités suivantes : 77

- l'évaluation annuelle 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 ; 78

- la remise à la direction, en temps utile, de rapports sur les modifications importantes de l'évaluation du risque de *compliance* ; 79

- la remise à l'organe responsable de la haute direction 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 de la société d'audit ; 80

- la remise à la direction et à l'organe responsable de la haute direction, en temps utile, de rapports sur les manquements graves constatés en matière de *compliance* et les faits de grande portée 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. 81

VIII. Révision interne

A. Instauration

Chaque établissement est en principe tenu d'instaurer une révision interne. 82

Lorsque l'instauration d'une révision interne propre à l'établissement n'apparaît pas appropriée, les tâches de révision interne peuvent être confiées : 83

- à 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'une maison de titres ou d'un autre intermédiaire financier (par ex. une entreprise d'assurances) soumis à une surveillance étatique (pour les banques étrangères, dans le cadre de l'art. 4^{quinquies} LB) ; 84

- à une seconde société d'audit indépendante de celle de l'établissement ; ou 85

- à une société du groupe ou un tiers indépendant, à condition que la société d'audit confirme que cette société ou ce tiers dispose de compétences professionnelles et de ressources techniques et personnelles appropriées. 86

B. Positionnement hiérarchique et organisation

La révision interne est subordonnée à l'organe responsable de la haute direction ou à son comité d'audit et elle exécute les tâches de révision et de surveillance qui lui sont confiées en toute indépendance. Elle dispose d'un droit d'accès, de consultation et de contrôle illimité au sein de l'établissement et de ses entreprises devant être consolidées au sens du Cm 98. 87

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. 88

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 *International Standards for the Professional Practice of Internal Auditing* de l'Institute of Internal Auditors (IIA). 89

Le système de rémunération des collaborateurs de la révision interne ne doit pas comprendre d'éléments susceptibles de générer des conflits d'intérêts. 90

C. Tâches et responsabilités

La révision interne effectue des audits et des évaluations indépendants concernant le caractère approprié et l'efficacité de l'organisation de l'entreprise et des processus commerciaux et plus particulièrement concernant le SCI et la gestion des risques de l'établissement. 91

Elle procède au moins une fois par an à une évaluation approfondie des risques encourus par l'établissement concernant les catégories de risques importantes au sens du Cm 53, en tenant dûment compte des évolutions externes (par ex. contexte économique, modifications réglementaires) et des facteurs internes (par ex. projets importants, orientation de l'activité). La révision interne des établissements participant au régime des petites banques selon les art. 47*a* à 47*e* OFR peuvent réaliser cette évaluation tous les deux ans dans la mesure où leur profil de risque n'a pas changé de manière importante. 92*

Sur la base de cette évaluation des risques et des autres besoins en matière d'audit, la révision interne fixe les objectifs d'audit et la planification de l'audit de la période d'audit suivante et demande à l'organe responsable de la haute direction ou à son comité d'audit 93

de les approuver ainsi que d'autres changements importants.

La révision interne s'assure que la direction et la société d'audit soient informées de l'évaluation des risques et des objectifs d'audit. 94

La révision interne rend compte à l'organe responsable de la haute direction 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. 95

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 haute direction ou à son comité d'audit, à la direction et à la société d'audit pour information. 96

En outre, la révision interne ou une autre instance indépendante au sein de l'établissement (par ex. fonction de *compliance* ou contrôle des risques) informe au moins une fois par semestre l'organe responsable de la haute direction ou son comité d'audit des corrections apportées aux insuffisances importantes et de l'état d'avancement de la mise en œuvre des recommandations de la révision interne et de la société d'audit. 97

IX. Structures de groupe

Cette circulaire s'applique par analogie aux groupes et conglomérats financiers (« groupes »). 98

Les groupes doivent régler les tâches et les responsabilités des unités ayant une responsabilité globale pour la conduite du groupe. Tout en tenant compte de l'activité commerciale et des principaux risques au niveau du groupe et de l'établissement individuel, les prescriptions doivent garantir la conduite efficace et uniforme du groupe, autoriser l'échange d'informations correspondant, tenir compte des structures juridiques et organisationnelles et définir les tâches et responsabilités ainsi que l'indépendance nécessaire des niveaux de conduite respectifs. Il convient en particulier de prendre en compte les risques résultant du regroupement de plusieurs entreprises en une entité économique unique. 99

X. Dispositions transitoires

Abrogé 100*-104*

Les dispositions étendues sur l'agrégation des données de risque et les rapports sur les risques selon le Cm 59 pour les banques d'importance systémique s'appliquent : 105

- à l'entrée en vigueur de cette circulaire, ou
- après un délai de transition de trois ans suivant la qualification de banque d'importance systémique selon l'art. 8 al. 3 LB (la date la plus tardive des deux s'applique).

Liste des modifications

La présente circulaire est modifiée comme suit :

Modifications du 31 octobre 2019 entrant en vigueur le 1er janvier 2020.

Cm modifiés	10, 41, 43, 45, 46, 52, 53, 54, 69, 71, 92
Cm abrogés	100, 101, 102, 103, 104
Autre modification	modification du titre avant le Cm 52

Avec l'entrée en vigueur de la législation liée à la LSFin et la LEFin au 1er janvier 2020, les renvois et notions y relatifs ont été adaptés.