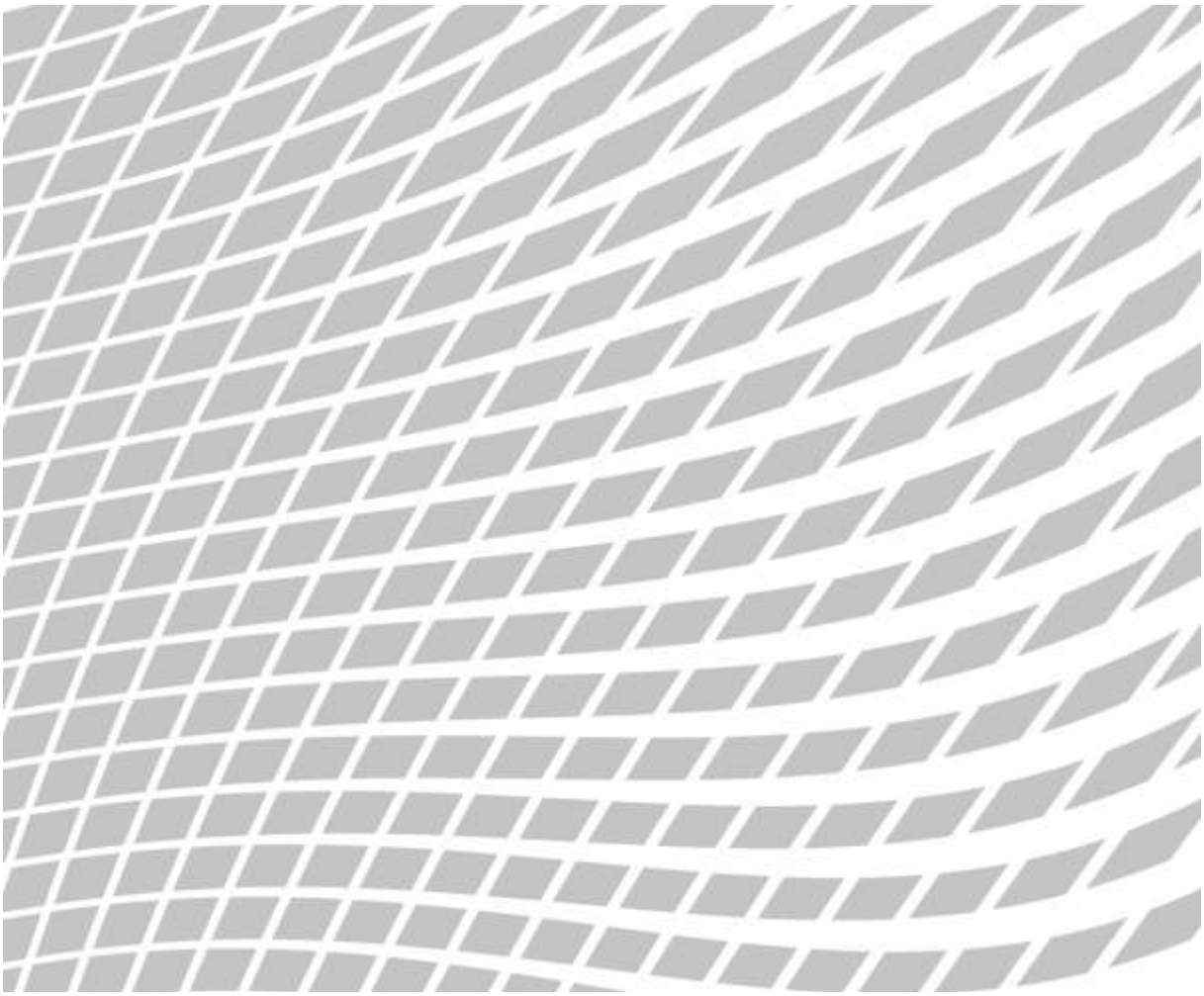
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

1er mars 2016

Circulaire 2016/x « Gouvernance d'entreprise – banques »

Rapport explicatif (révision totale de la Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » ; révision partielle de la Circ.-FINMA 08/21 « Risques opérationnels – banques » ; révision partielle de la Circ.-FINMA 10/1 « Systèmes de rémunération »)



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

Table des matières

Eléments essentiels **4**

1 Contexte **5**

2 Besoin de réglementation et objectif **7**

3 Explications relatives à la Circ.-FINMA 16/x « Gouvernance d'entreprise – banques » **8**

3.1 Objet, définitions et champ d'application 8
3.2 Organe responsable de la direction supérieure 9
3.2.1 Catalogue des tâches 9
3.2.2 Composition 9
3.2.3 Indépendance 10
3.2.4 Gestion du mandat 10
3.2.5 Comités 11
3.3 Direction 11
3.4 Concept-cadre pour la gestion des risques à l'échelle de l'établissement 12
3.5 Système de contrôle interne 14
3.6 Révision interne 15
3.7 Structures de groupe 16
3.8 Publication 16
3.9 Dispositions transitoires 17

4 Explications relatives à la révision partielle de la Circ.-FINMA 08/21 « Risques opérationnels – banques » **18**

4.1 Principe de proportionnalité au chapitre IV. Exigences qualitatives concernant la gestion des risques opérationnels 18
4.2 Simplification du chapitre IV. Exigences qualitatives concernant la gestion des risques opérationnels 18

4.3 Intégration de principes concernant les risques informatiques et les cyberrisques 19
4.4 Maintien des prestations critiques en cas d'insolvabilité 20
4.5 Risques dans les activités financières transfrontières 20
4.6 Annexe 3 : Traitement des données électroniques de clients 21

5 Explications relatives à la révision partielle de la Circ.-FINMA 10/1 « Systèmes de rémunération » 21

6 Conséquences 22

7 Suite de la procédure 23

Eléments essentiels

La FINMA soumet la Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » à une révision totale. Cette circulaire a été édictée par la CFB en 2006 et n'a guère été adaptée depuis. Elle ne reflète pas les évolutions fondamentales dans le domaine de la gouvernance d'entreprise et les enseignements importants concernant la gestion des risques qui ont été tirés de la crise des marchés financiers. Les organismes internationaux de normalisation, notamment le Comité de Bâle sur le contrôle bancaire, ont entre-temps adapté leurs directives pour une gouvernance d'entreprise moderne et une gestion des risques efficace. La FINMA profite de la révision des normes internationales pour remanier intégralement la Circ.-FINMA 08/24. Ainsi, elle tient également compte des recommandations du Fonds monétaire international formulées dans le cadre du « Programme d'évaluation du secteur financier » en 2014.

Concrètement, les nouveautés et adaptations suivantes ont été prévues :

1. Des principes et des structures destinés au pilotage de la banque *(« checks and balances »)* sont introduits pour l'organe responsable de la direction supérieure et la direction, en plus des aspects liés au contrôle. La FAQ sur la direction supérieure est en grande partie intégrée dans la circulaire.

2. Les banques des catégories de surveillance 1 à 3 devront désormais mettre en place un comité d'audit et un comité des risques séparés.

3. Tous les établissements doivent disposer d'un concept-cadre pour la gestion des risques élaboré par la direction et adopté par l'organe responsable de la direction supérieure.

4. Toutes les banques des catégories de surveillance 1 à 3 doivent entretenir un contrôle des risques sous la houlette du CRO. Pour les banques des catégories de surveillance 1 et 2, le CRO doit faire partie de la direction.

5. Des prescriptions minimales concernant la publication dans le domaine de la gouvernance d'entreprise sont fixées pour toutes les banques. Les banques des catégories de surveillance 1 à 3 sont soumises à une obligation de publication étendue fondée sur les directives de SIX concernant les informations relatives à la *corporate governance*.

La Circ.-FINMA 08/21 « Risques opérationnels – banques » et la Circ.-FINMA 10/1 « Systèmes de rémunération » font l'objet d'une révision partielle dans le cadre de la révision totale de la Circ.-FINMA 08/24.

La Circ.-FINMA 08/21 est allégée au chapitre des exigences qualitatives concernant la gestion des risques des éléments qui sont désormais intégrés dans la Circ.-FINMA « Gouvernance d'entreprise – banques » en guise d'exigences « supérieures ». Le principe de la gestion des risques concernant l'infrastructure technologique est en outre complété par les aspects des risques informatiques et des

cyberrisques et un nouveau principe concernant les risques dans les activités financières transfrontières est introduit. Le principe de la continuité en cas d'interruption de l'activité est en outre enrichi de prescriptions concernant le maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique.

L'application obligatoire de la Circ.-FINMA 10/1 doit être limitée aux banques disposant de fonds propres minimaux supérieurs à 10 milliards de francs. Des modifications mineures sont en outre apportées aux exigences concernant la conception des systèmes de rémunération dans la circulaire.

1 Contexte

La Commission fédérale des banques a fait entrer en vigueur l'actuelle Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » le 1er janvier 2007. Cette circulaire définit les exigences relatives au système de contrôle interne et à la gouvernance d'entreprise des banques, notamment en ce qui concerne l'organe responsable de la direction supérieure et la direction, la révision interne, la fonction de *compliance* et le contrôle des risques.

A la date de son édiction, la Circ.-FINMA 08/24 reflétait les connaissances et la pratique de l'époque en matière de surveillance et de contrôles internes des banques. Depuis cette date, seuls des ajustements ponctuels ont été apportés à la circulaire. La circulaire ne reflète ni les leçons tirées de la crise des marchés financiers ni les récentes évolutions dans le domaine de la gouvernance d'entreprise.

Les faiblesses dans la gestion des risques et dans la gouvernance d'entreprise des banques ont considérablement aggravé la situation lors de la crise des marchés financiers. Des déficits ont été décelés à différents niveaux de la gestion des risques, par exemple en matière d'identification, de mesure et de communication des risques. Il est dès lors apparu que les organes de conduite des banques avaient des connaissances techniques insuffisantes concernant le traitement et la maîtrise des risques. Les dysfonctionnements ont en outre été amplifiés par des systèmes de rémunération comportant des incitations inappropriées.

Différents organismes internationaux de normalisation ont renforcé leurs attentes à l'égard de la gouvernance d'entreprise ces dernières années. Les « Principes de gouvernement d'entreprise du G20 et de l'OCDE » (novembre 2015) et les « Principes de gouvernance d'entreprise à l'intention des banques » du Comité de Bâle sur le contrôle bancaire (juillet 2015) sont particulièrement déterminants pour le secteur financier.

Le Comité de Bâle a par ailleurs mis à jour les principes directeurs pour un pilotage, une administration et un contrôle appropriés de certaines catégories de risques dans le cadre de l'agenda des réformes de Bâle III. A cet égard, la FINMA a repris les principes bâlois concernant la gestion des risques opérationnels en 2013, en les transposant dans la Circ.-FINMA 08/21 « Risques opérationnels – banques ». Il existe certains recoupements avec les réglementations actuelles en matière de contrôle des risques dans la Circ.-FINMA 08/24.

La Suisse a été contrôlée par le Fonds monétaire international (FMI) en 2014, dans le cadre du « Programme d'évaluation du secteur financier ». Le FMI a notamment émis les recommandations suivantes concernant la réglementation de la gouvernance d'entreprise et la gestion des risques :

- prescriptions explicites et condensées concernant les éléments qualitatifs de la gestion et du contrôle des risques dans la perspective de l'entreprise globale, l'établissement de rapports sur les risques à l'échelle de l'établissement, l'analyse intégrale des données de risques agrégées et une meilleure coordination entre l'appétence au risque et la stratégie en matière de risques ;
- clarté accrue des prescriptions concernant les connaissances techniques spécifiques aux risques des membres du conseil d'administration ;

- renforcement de la proportion des membres du conseil d'administration ayant une indépendance suffisante vis-à-vis du propriétaire, notamment dans l'optique des banques en mains de corporations de droit public ;
- amélioration de la position et du profil du CRO dans l'entreprise ;
- introduction de règles pour des comités des risques séparés ayant des connaissances spécifiques en matière de risques ;
- introduction de prescriptions pour une évaluation interne à la banque des nouveaux domaines d'activité, produits et structures modifiées de l'entreprise.

Les recommandations citées dont la FINMA soutient le principe doivent être concrétisées dans le cadre de la révision totale de la Circ.-FINMA 08/24.

Les risques informatiques, et plus particulièrement les cyberrisques, ont fortement augmenté ces dernières années, dans le sillage des progrès techniques qui donnent lieu à une numérisation accrue des transactions financières et à une externalisation plus importante des processus et des prestations de service à des tierces parties. L'échange avec les spécialistes met en lumière le potentiel de risque élevé et les défis considérables auxquels est confrontée la place financière suisse. La FINMA a déjà étudié de près cette thématique et engagé différentes mesures afin de pouvoir évaluer le traitement des assujettis présentant de tels risques[1]. Pour cette raison et en coordination avec les efforts internationaux, la FINMA juge nécessaire l'introduction de principes concernant les risques informatiques et les cyberrisques dans la Circ.-FINMA 08/21, afin de garantir le respect des principes fondamentaux dans le traitement de ces risques sur l'ensemble des établissements.

La garantie du maintien des fonctions et prestations critiques en cas d'insolvabilité constitue une exigence critique, notamment à l'égard des banques d'importance systémique. Le Conseil de stabilité financière (CSF) a bouclé une consultation sur des exigences allant dans ce sens début 2016. La FINMA estime qu'il est nécessaire d'ajouter à la Circ.-FINMA 08/21 un principe concernant la garantie de la continuité en cas d'insolvabilité.

Le modèle d'affaires de nombreuses banques de gestion de fortune est traditionnellement focalisé sur les prestations transfrontières pour une clientèle privée résidant à l'étranger. Les risques juridiques et de réputation induits par cette activité ont fortement augmenté ces dernières années. La FINMA a expliqué sa position concernant cette thématique dans un document de position en octobre 2010. Un principe consacré à cette question doit désormais être intégré à la Circ.-FINMA 08/21.

[1] Il est par exemple possible d'effectuer des audits supplémentaires selon la Circ.-FINMA 2013/03 « Activités d'audit » ou une évaluation interne concernant la gestion des cyberrisques.

2 Besoin de réglementation et objectif

La FINMA considère qu'il est indispensable d'aligner les prescriptions concernant la mise en place d'une gouvernance d'entreprise solide et d'une gestion efficace des risques dans les banques et les négociants en valeurs mobilières sur les principales directives actuelles des organismes internationaux de normalisation. Les exigences qualitatives concernant la gestion des risques, et plus particulièrement la gouvernance des risques, doivent être détachées des circulaires spécifiques aux risques pour être regroupées dans la Circ.-FINMA « Gouvernance d'entreprise – banques ». Celle-ci doit également intégrer les aspects relatifs à l'organe responsable de la direction supérieure contenus dans la FAQ. La pratique vécue par la surveillance des banques ces dernières années doit ainsi être consolidée et la sécurité juridique doit être renforcée.

Dans certains domaines, la Circ.-FINMA 08/24 n'est pas conforme à l'objectif d'une réglementation fondée sur des principes. Ces passages doivent être combinés ou abrogés purement et simplement.

Les dispositions en matière de surveillance concernant la gestion des risques à l'échelle de l'établissement ainsi que les tâches et les responsabilités de la direction doivent notamment être redéfinies dans le cadre de la révision totale de la Circ.-FINMA 08/24. Une représentation globale de ces exigences dans la nouvelle Circ.-FINMA « Gouvernance d'entreprise – banques » permet de simplifier, dans le cadre d'une révision partielle, les exigences qualitatives en matière de gestion des risques dans la Circ.-FINMA 08/21.

La révision de la Circ.-FINMA 08/21 offre en outre la possibilité d'intégrer des thématiques essentielles pour les risques opérationnels, tels que les risques informatiques et les cyberrisques, le maintien des prestations critiques en cas d'insolvabilité et la prise en compte des risques dans les activités financières transfrontières *(crossborder)*. La révision partielle de la Circ.-FINMA 08/21 doit en outre uniformiser l'application du principe de proportionnalité.

La FAQ relative à la Circ.-FINMA 08/21 et la FAQ « Risques juridiques et de réputation dans le cadre des activités financières transfrontières » doivent par ailleurs être intégrées dans la Circ.-FINMA 08/21 dans le cadre de la révision partielle, pour autant que cela soit jugé utile.

L'introduction des principes relatifs aux risques informatiques et aux cyberrisques doit enrichir le principe existant concernant l'infrastructure technologique en conformité avec les efforts internationaux. Ces principes doivent garantir le respect des principes fondamentaux concernant le traitement de ces risques à l'échelle de l'établissement.

L'intégration du maintien des prestations critiques en cas d'insolvabilité doit être réalisée dans le cadre d'une extension du principe actuel concernant la continuité en cas d'interruption des affaires qui garantit le maintien et la poursuite des prestations critiques en cas d'insolvabilité. Elle est conforme aux évolutions de la réglementation internationale dans ce domaine.

Le document de position de la FINMA sur les risques dans le cadre des activités financières transfrontières doit être résumé dans un principe séparé parmi les exigences qualitatives concernant le traite-

ment des risques opérationnels. L'approche fondée sur les risques qui avait été poursuivie jusqu'à présent doit continuer à s'appliquer. Les risques juridiques qui peuvent cependant être associés à d'importants risques de réputation à l'instar d'autres catégories de risques tiennent ici lieu de critère de base.

Pour finir, la Circ.-FINMA 10/1 « Systèmes de rémunération » doit également être mise à jour en relation avec les évolutions dans le domaine de la gouvernance d'entreprise. En dehors de quelques ajustements mineurs, la mise en œuvre contraignante doit être limitée aux banques d'importance systémique et à quelques établissements désignés par la FINMA. L'on a ainsi l'assurance que le champ d'application de la circulaire se limitera aux établissements présentant des systèmes de rémunération complexes et offrant des rémunérations d'un montant matériellement significatif.

3 Explications relatives à la Circ.-FINMA 16/x « Gouvernance d'entreprise – banques »

La nouvelle circulaire doit pouvoir être lue et comprise en toute autonomie. Pour cette raison, certains chiffres marginaux reprennent des dispositions de textes réglementaires plus généraux pour une meilleure compréhension.

Dans le présent projet de circulaire, certains passages ont été surlignés. Les couleurs renvoient à la provenance du texte. Sont surlignés en jaune les passages repris de la Circ.-FINMA 08/24 avec de légers ajustements. Les parties issues des Circ.-FINMA 08/21 et 08/32 apparaissent en rouge. Le bleu signale les textes émanant d'organismes internationaux de normalisation. Quant au vert, il signale les chiffres marginaux dont la teneur provient de la FAQ sur la direction supérieure.

3.1 Objet, définitions et champ d'application

La Circ.-FINMA 08/24 actuelle se focalise sur la surveillance de l'activité commerciale ainsi que sur les contrôles internes et leur surveillance. La révision totale élargira la perspective de la circulaire en ce sens qu'elle introduira des exigences fondamentales à l'égard de la gouvernance interne et de la gestion des risques des banques et des négociants en valeurs mobilières, en plus des exigences relatives au système de contrôle interne (SCI).

Le champ d'application thématiquement étendu requiert une définition et une délimitation des termes employés. Les notions définies dans la circulaire visent à en assurer la compréhension en vue d'une concrétisation en bonne et due forme des différentes exigences. Il n'y a aucun droit à une application des présentes définitions en dehors du champ de la circulaire.

Les exigences dans la circulaire sont fondées sur des principes. Leur mise en œuvre doit dépendre au cas par cas de la taille, de la complexité, de la structure et du profil de risque de l'établissement. La gouvernance d'entreprise et la gestion des risques sont des thèmes de surveillance impossibles à contrôler et à surveiller dans le cadre d'une approche de type *« one size fits all »*. Les spécificités et

risques des établissements individuels doivent être pris en compte dans la pratique en matière de surveillance comme précédemment. Pour que les nouveaux principes d'application parfois plus étendus ne débouchent pas sur un excès de réglementation, les banques et les négociants en valeurs mobilières des catégories de surveillance 4 et 5 sont en outre explicitement exemptés de la mise en œuvre de certaines exigences.

L'application systématique du principe de proportionnalité remplace l'approche *« comply or explain »* jusqu'à présent utilisée à certains endroits de la circulaire. Ce principe éprouvé sur le marché selon lequel le non-respect de prescriptions d'autorégulation doit être expliqué dans le rapport de gestion est rarement appliqué dans le domaine réglementaire et complique, dans la pratique, la surveillance permanente des établissements. Si les exigences ne peuvent pas être concrétisées dans des cas particuliers spécifiquement justifiés, des autorisations d'exception doivent être utilisées à l'avenir. C'est déjà en partie le cas dans la pratique, puisque l'organisation de l'organe responsable de la direction supérieure et des fonctions de pilotage et de contrôle à l'échelle de l'établissement est généralement présentée dans des règlements soumis à autorisation, par exemple la règle du tiers concernant l'indépendance de l'organe responsable de la direction supérieure ou la mise en place d'un comité d'audit de l'organe responsable de la direction supérieure.

3.2 Organe responsable de la direction supérieure

3.2.1 Catalogue des tâches

Le profil de l'organe responsable de la direction supérieure doit être renforcé de manière ciblée. Les interventions dans la liberté d'organisation de l'établissement se limitent aux nécessités du droit de la surveillance. Le rôle de l'organe responsable de la direction supérieure en tant que principale barrière de l'établissement contre les risques est notamment clarifié. Le catalogue des tâches est par ailleurs étendu à toutes les compétences de base selon le droit de la société anonyme (cf. l'art. 716*a* al. 1 CO) au-delà de la perspective du contrôle. L'ancrage dans le droit de la société anonyme est conforme à la pratique en vigueur en matière de surveillance dont la teneur se fonde en principe sur le catalogue des attributions du droit de la société anonyme.

3.2.2 Composition

Une composition équilibrée de l'organe responsable de la direction supérieure est particulièrement importante, en dehors du nombre minimum de ses membres – un nombre minimum de trois s'applique aux banques (art. 11 al. 1 OB). L'organe responsable de la direction supérieure doit être composé de manière suffisamment diversifiée pour que tous les autres domaines centraux tels que la finance et la comptabilité, la gestion des risques, la *compliance*, le *controlling* et l'informatique soient représentés avec les compétences requises, et ce, en plus des principales activités commerciales. Cela ne veut pas dire pour autant que chaque membre doit avoir plusieurs années d'expérience dans le secteur bancaire. Chaque membre dispose cependant d'au moins une connaissance approfondie qui contribue à l'équilibre de l'organe collectif.

Si ce principe de la diversité est appliqué de façon crédible, de bonnes connaissances en matière de finance et de comptabilité et une expérience de l'activité d'audit doivent être dûment représentées au sein de l'organe. La règle actuelle,[2] selon laquelle un ou deux administrateurs qualifiés ayant une expertise spécifique doivent se voir confier les tâches d'un comité d'audit au cas où celui-ci ferait défaut, ne s'appliquera donc plus à l'avenir.

L'exigence d'une composition équilibrée signifie également que l'organe dans son ensemble est suffisamment familier avec le rayon d'action et les marchés cibles de l'établissement ou du groupe. Ainsi, dans le cas d'un établissement à vocation régionale ou nationale, une part importante des membres doit entretenir une relation étroite avec la Suisse, en raison de leur lieu de vie, de leur carrière professionnelle ou de leur formation, alors qu'un périmètre de recrutement mondial peut être retenu pour les groupes actifs à l'échelle internationale.

3.2.3 Indépendance

Le principe de la séparation des pouvoirs entre l'organe responsable de la direction supérieure et la direction reste déterminant pour le secteur bancaire. Un tiers au moins des membres de l'organe responsable de la direction supérieure ne doit notamment entretenir aucune proximité particulière avec l'établissement. Contrairement au principe actuel *« comply or explain »* (cf. 3.1 ci-dessus), la règle du tiers doit désormais être plus contraignante. Dans des cas particuliers justifiés, la FINMA peut cependant accorder des allègements, par exemple aux petites entreprises durant la phase de démarrage.

Indépendance signifie aussi distance par rapport au propriétaire, notamment vis-à-vis des gros actionnaires. Il faut s'assurer qu'une partie importante des membres ne détienne pas une participation qualifiée dans l'établissement et ne représente pas une personne détenant une participation qualifiée. La formulation du degré d'indépendance requis est délibérément ouverte. Dans certaines situations, une indépendance majoritaire est requise, alors qu'une représentation majoritaire du groupe dans la filiale bancaire est tout à fait envisageable, par exemple, dans des structures de groupes purement suisses. La diversité rencontrée dans la pratique demande du discernement et, dans des cas particuliers, des solutions sur mesure.

3.2.4 Gestion du mandat

Les principes essentiels de la gestion du mandat sont transposés de la FAQ « Direction supérieure des banques et des négociants en valeurs mobilières » à la présente circulaire. Il est cependant sciemment renoncé à l'introduction d'un plafond rigide visant à limiter le nombre de mandats multiples. L'on attend toutefois un engagement actif et approprié de la part de chaque membre. Les différents membres de l'organe responsable de la direction supérieure doivent s'assurer de consacrer suffisamment de temps à leur mandat pour l'exercer avec diligence. Les conflits d'intérêts avec l'établissement doivent être évités autant que possible. Les membres de l'organe responsable de la direction supérieure doivent également se tenir durablement à disposition lors des situations de crise et d'urgence.

[2] Circ.-FINMA 08/24, Cm 30.

Leur disponibilité ne se limite pas au rythme ordinaire des séances. Les attentes à l'égard du président de l'organe responsable de la direction supérieure dont la position particulièrement éminente est aussi déterminante selon le droit de la surveillance ont également été reprises de la FAQ.

3.2.5 Comités

L'instauration contraignante d'un comité d'audit pour les banques d'une certaine importance (catégories de surveillance 1 à 3) et l'introduction d'un comité des risques séparé pour les banques de ces catégories figurent parmi les nouveautés prévues. En mettant sur un pied d'égalité réglementaire le comité d'audit et le comité des risques, la proposition se conforme aux prescriptions du Comité de Bâle qui recommande vivement de tels comités pour les banques les plus importantes et les prévoit obligatoirement pour les banques d'importance systémique. L'introduction d'un comité des risques séparé tient également compte de la critique formulée dans le cadre du PESF qui décelait des déficits en matière de connaissances spécialisées spécifiques aux risques au niveau de la direction supérieure précisément dans les banques de taille moyenne. Eu égard aux différences en termes de point de vue et d'orientation entre ces deux comités, ils doivent en outre se différencier par leur composition.

A une exception près, toutes les banques des catégories 1 à 3 possèdent aujourd'hui un comité d'audit. Les comités des risques ne constituent en revanche pas encore la règle dans le secteur bancaire suisse. Parmi les banques de catégorie 3, à peine la moitié possède un comité des risques séparé et environ un tiers une version combinée (comité d'audit et des risques commun).

La composition en bonne et due forme d'un comité d'audit et des risques implique que ses membres soient majoritairement indépendants et possèdent les connaissances techniques ainsi que l'expérience requises dans la spécialité. Les présidents des comités d'audit et des risques doivent également être indépendants et ne doivent présider ni l'organe responsable de la direction supérieure ni un quelconque autre comité. Le président de l'organe responsable de la direction supérieure ne devrait en outre pas être membre du comité d'audit.

Les banques d'importance systémique doivent par ailleurs instaurer un comité des rémunérations et des nominations séparé, en référence aux normes du Comité de Bâle.

3.3 Direction

Les dispositions relatives à la direction dans la version applicable de la Circ.-FINMA 08/24 se limitent à des explications quant à la mise en œuvre des prescriptions de l'organe responsable de la direction supérieure concernant la mise en place, le maintien et la validation régulière du contrôle interne, au système d'information du management (MIS) et à la définition de la structure d'organisation correspondante.

La nouvelle circulaire a été enrichie à cet égard et contient désormais les principales tâches et responsabilités attribuées à la direction : la conduite des affaires courantes et la représentation de l'établissement vis-à-vis des tiers dans le secteur opérationnel, la formulation de propositions concer-

nant les affaires qui relèvent de la compétence ou nécessitent l'approbation de l'organe responsable de la direction supérieure, la définition d'une structure de conduite et d'organisation à l'échelle de l'établissement, y compris l'entretien d'un système d'information du management et d'un système de contrôle interne ainsi que le pilotage opérationnel des revenus et des risques.

La FINMA exigeait déjà jusqu'à présent de la direction qu'elle assume ces tâches et ces responsabilités dans le cadre de l'approbation des statuts et des règlements internes. La pratique incontestée et de longue date en matière d'autorisation est ainsi transposée dans une circulaire.

Le présent projet contient désormais aussi des dispositions concernant les exigences à l'égard des membres de la direction. Aux termes de l'art. 3 al. 2 let. c LB, ils doivent jouir d'une bonne réputation et présenter toutes les garanties d'une activité irréprochable. Autrement dit, les membres de la direction en tant qu'organe collectif disposent de l'expérience nécessaire dans les secteurs bancaire et financier, sont intègres et disposent des compétences de gestion suffisantes. En outre, chacun d'entre eux en tant que responsable d'une fonction possède les connaissances techniques requises. La direction doit par ailleurs assumer son rôle de modèle et incarner la culture d'entreprise et du risque par son comportement personnel *(« tone at the top »)*.

La section « Séparation des fonctions et activités de contrôle » a en revanche été purement et simplement abrogée, dans le sens d'une réglementation fondée sur des principes.

3.4 Concept-cadre pour la gestion des risques à l'échelle de l'établissement

La Circ.-FINMA « Gouvernance d'entreprise – banques » reprend les exigences qualitatives en matière de gestion des risques aujourd'hui définies dans la Circ.-FINMA 08/21 pour la gestion des risques opérationnels, pour tous les types de risques.

Le concept-cadre est généralement constitué d'un document principal ainsi que d'autres prescriptions internes et englobe notamment la politique de risque, l'appétence au risque ainsi que les prescriptions relatives aux limites (et valeurs-seuils) permettant de respecter l'appétence au risque.

Il correspond souvent à la pratique déjà vécue aujourd'hui selon laquelle il existe des prescriptions et des directives concernant les différents aspects du concept-cadre et que celles-ci ont (en partie) été approuvées par l'organe responsable de la direction supérieure. Dans certains établissements, ces aspects et le concept-cadre doivent cependant être consolidés et approuvés par l'organe responsable de la direction supérieure en raison de la nouvelle circulaire.

La politique de risque se définit au travers de la stratégie en matière de risques qui fixe les conditions-cadres pour l'identification, la mesure, l'administration et la surveillance des risques ainsi que pour l'établissement de rapports sur les risques et qui garantit ainsi le respect des limites posées en matière de risques. Les instruments nécessaires à la mise en œuvre de la stratégie en matière de risque sont par exemple définis en plus d'une organisation structurelle et fonctionnelle pour la gestion des risques dans l'établissement.

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 inclut la perspective du risque au niveau agrégé mais aussi au niveau des principales catégories de risques, c.-à-d. les risques auxquels est exposé l'établissement classés par natures[3], types[4] et niveaux[5].

La détermination des limites posées en matière de risques se fonde sur l'appétence au risque, c.-à-d. aussi bien sur la perspective du risque agrégé que par rapport aux catégories de risques respectives. Les limites jouent un rôle de pilotage. Des valeurs-seuils doivent également être prévues en amont afin de permettre une identification précoce de la violation (éventuelle) des limites posées en matière de risques. En cas de dépassement des limites, l'organe responsable de la direction supérieure doit en être immédiatement informé afin d'engager des stratégies et des instruments de réduction des risques qui permettront de garantir rapidement le respect des limites posées en matière de risques ou d'approuver un dépassement temporaire de ces limites.

Le concept-cadre inclut des principes régissant l'élaboration d'une documentation permettant de soumettre la détermination de l'appétence au risque et des limites posées en matière de risques à une évaluation et à une vérification indépendantes appropriées, tant par l'organe responsable de la direction supérieure que par d'autres instances de contrôle. Ces principes incluent notamment des prescriptions autorisant la traçabilité des évaluations des risques et des principes utilisés à cet effet pour la détermination de l'appétence au risque et des limites posées en matière de risques. Cette documentation peut par exemple se fonder sur une analyse des risques annuelle à l'échelle de l'établissement ou se référer aux méthodes et/ou modèles de mesure des risques utilisés.

Les systèmes d'établissement de rapports sur les risques et d'information du management (MIS) correspondent à un *reporting* à des fins de surveillance et d'information, pour des groupes d'ayants droit tant internes qu'externes.

En dépit du caractère stratégique du concept-cadre, celui-ci doit être adapté rapidement à toute situation nouvelle, en cas de changements importants, par exemple en cas de modification de l'activité commerciale de l'établissement, du marché ou de la loi ainsi que du droit de la surveillance. Le concept-cadre est en principe contrôlé à intervalles réguliers par l'organe responsable de la direction supérieure. Il doit par ailleurs être soumis à un contrôle et à une adaptation continus et rapides par une unité d'organisation clairement désignée et disposant de personnel qualifié en quantité suffisante. Cette unité d'organisation correspond typiquement au contrôle des risques ou à la fonction de *compliance* qui, en leur qualité d'instances de contrôle indépendantes et dans la perspective de leur participation au processus de développement *(new business process)* ou à l'examen de la diligence *(due diligence)*, soutiennent l'organe responsable de la direction supérieure dans son contrôle périodique du concept-cadre. La révision interne assure en outre un contrôle régulier, indépendant et global du

[3] Par exemple risques de crédit, de marché, de liquidités, opérationnels, etc.

[4] Par exemple perte attendue, *value-at-risk*, critères internes de mesure des liquidités, etc.

[5] Par exemple produits, départements de l'entreprise, engagements pays, etc.

concept-cadre dans la perspective de sa définition et de son respect ainsi que de sa mise en œuvre en tant qu'élément du système de contrôle interne.

Les prescriptions du concept-cadre doivent s'appliquer dans tout l'établissement. Autrement dit, la prise en compte des prescriptions dans le cadre d'un processus de développement *(new business process)* ou d'un examen de la diligence *(due diligence)*, par exemple en cas de modifications de l'organisation telles que des externalisations, des fusions ou des acquisitions ou l'examen de nouveaux domaines d'activité et produits, doit notamment être garantie, parallèlement à l'application des principes aux structures existantes.

Des dispositions supplémentaires relatives à l'agrégation des données de risque et à l'établissement de rapports sur les risques doivent en outre être définies pour les banques d'importance systémique. Ces dispositions doivent être prévues en tant que partie intégrante du concept-cadre pour la gestion des risques à l'échelle de l'établissement et doivent donc être développées et mises en œuvre par la direction et approuvées par l'organe responsable de la direction supérieure. Les dispositions relatives à l'agrégation des données de risque et à l'établissement de rapports sur les risques incluent des exigences à l'égard de l'architecture des données et de l'infrastructure informatique, ce qui permet notamment d'identifier les risques de concentration[6]. Il est essentiel à cet égard de rechercher une architecture des données et une infrastructure informatique aussi flexibles que possible, afin de permettre une prise en compte et une intégration rapide des nouvelles analyses de scénarios et simulations de crise.

3.5 Système de contrôle interne

La révision de la Circ.-FINMA 08/24 vise à introduire un système de contrôle interne (SCI) global. La mise en œuvre effective du concept-cadre pour la gestion des risques à l'échelle de l'établissement et plus particulièrement le respect de l'appétence au risque adopté par l'organe responsable de la direction supérieure et des limites posées en matière de risques correspondantes doivent être assurés à cet égard.

Dans sa globalité, le SCI est constitué d'au moins trois instances de contrôle indépendantes les unes des autres, à savoir les unités d'affaires génératrices de revenus, les instances de contrôle indépendantes des unités d'affaires génératrices de revenus et la révision interne.

Le contrôle des risques et la fonction de *compliance* représentent les principales instances de contrôle indépendantes. D'autres instances de contrôle indépendantes peuvent être définies en fonction de la taille, de la complexité de l'activité et de l'organisation et du profil de risque d'un établissement. Si un établissement dispose d'une unité d'organisation séparée qui se consacre à des thématiques globales en matière de sécurité, telles que la protection de l'information, des personnes et des objets, ou s'il possède un contrôle financier indépendant au plan organisationnel, ceux-ci peuvent faire office d'instance de contrôle indépendante distincte, parallèlement au contrôle des risques et à la fonction de *compliance*. Dans tous les cas, les différentes responsabilités des instances de contrôle doivent toute-

[6] Par exemple au niveau des pays, des contreparties, etc.

fois être clairement définies et communiquées. En d'autres termes, il s'agit notamment de définir qui prend et administre les risques et qui est responsable de la surveillance de ces risques, indépendamment d'une composante de revenu. Les tâches des instances de contrôle indépendantes doivent par ailleurs être assumées, tant au niveau du groupe que de l'établissement individuel.

Les dispositions remaniées concernant un SCI global se focalisent principalement sur le contrôle des risques qui assure une surveillance de l'appétence au risque et des limites posées en matière de risques (selon le concept-cadre pour la gestion des risques à l'échelle de l'établissement) indépendante des unités d'affaires génératrices de revenus. Les exigences remaniées concernant l'instauration et la subordination du contrôle des risques prévoient l'application du principe de proportionnalité, ce qui signifie que l'instauration et la subordination doivent varier en fonction de la catégorie de surveillance. Concrètement, cela signifie que les établissements des catégories de surveillance 1 à 3 doivent disposer d'un Chief Risk Officer (CRO) autonome, qui est au minimum responsable du contrôle des risques. Dans les banques d'importance systémique (catégories de surveillance 1 et 2), il est en outre impératif que le CRO fasse partie de la direction. Ce n'est pas une obligation pour les établissements de la catégorie de surveillance 3. Dans les établissements des catégories de surveillance 4 et 5, le contrôle des risques peut en outre être regroupé avec d'autres fonctions de la banque (par exemple avec la fonction de *compliance*) ou assumée par un collaborateur employé parallèlement à une autre fonction, pour autant que cela paraisse approprié dans l'optique de la garantie de l'indépendance et de la prévention des conflits d'intérêts[7]. Dans tous les cas, la fonction de *compliance* peut constituer une unité avec le service juridique, indépendamment de la catégorie de surveillance de l'établissement respectif. Les établissements des catégories de surveillance 4 et 5 peuvent en outre externaliser la fonction de *compliance*.

Le contrôle des risques informe immédiatement, c.-à-d. sans hésitation fautive, l'organe responsable de la direction supérieure des violations des limites posées en matière de risques approuvées par ce dernier dans le concept-cadre pour la gestion des risques à l'échelle de l'établissement.

3.6 Révision interne

Les dispositions relatives à la révision interne sont repositionnées dans le présent projet de circulaire et ne se trouvent désormais plus à la suite de celles relatives à l'organe responsable de la direction supérieure (conseil d'administration), mais après les réglementations relatives au système de contrôle interne, conformément au modèle SCI courant des trois lignes de défense *(three lines of defence)*.

Les explications antérieures concernant la révision interne sont réagencées en fonction de leur importance et légèrement adaptées. L'indépendance de la révision interne en tant que condition essentielle est ainsi soulignée et le profil d'exigences existant est renforcé. Les conditions du transfert des tâches de la révision interne à un tiers indépendant sont par ailleurs coordonnées avec le modèle de rapport d'audit prudentiel.

[7] Par exemple aucun regroupement ni aucun cumul des fonctions avec des unités d'affaires génératrices de revenus.

3.7 Structures de groupe

A l'exception des réglementations relatives au champ d'action de la révision interne dans les groupes financiers, la circulaire en vigueur ne comporte aucune disposition relative aux structures de groupe. Etant donné que la circulaire actuelle s'applique déjà par analogie aux structures de groupe dans la pratique en vigueur et que les directives internationales prévoient également des dispositions correspondantes, des prescriptions fondées sur des principes sont désormais intégrées dans la nouvelle circulaire.

Le projet ne prévoit ainsi aucune modification de la pratique en matière de surveillance et ne règle expressément que le fait que tous les principes et dispositions de la circulaire doivent s'appliquer par analogie aux groupes et conglomérats financiers, notamment aux unités ayant la responsabilité globale de la gestion du groupe, qu'il s'agisse d'une structure de holding, de maison mère ou d'une structure de groupe atypique.

3.8 Publication

La transparence des entreprises envers leurs parties prenantes est aujourd'hui reconnue comme un élément important d'une bonne gouvernance d'entreprise (OCDE, Comité de Bâle sur le contrôle bancaire, economiesuisse). Les grandes entreprises et les entreprises actives au plan international appliquent aujourd'hui tout naturellement les normes postulées aux plans national et international. Les entreprises qui appliquent une norme comptable reconnue au plan international sont en outre tenues de présenter en toute transparence des informations spécifiques sur la structure juridique de l'entreprise et sur la gestion des risques dans le rapport de gestion[8].

En Suisse, les entreprises cotées à la bourse SIX Exchange en Suisse sont tenues de publier certaines informations sur la gouvernance d'entreprise dans le rapport de gestion, et ce, conformément à la Directive Corporate Governance[9]. Dans le « Code suisse de bonnes pratiques pour le gouvernement d'entreprise », economiesuisse renvoie à l'applicabilité de la directive de SIX dans le chapitre « Publication ».

Les dispositions du droit de la société anonyme concernant la publication et qui sont concrétisées par la législation sur les banques s'appliquent en principe à toutes les banques en Suisse. En ce qui concerne la publication d'informations sur le thème de la gouvernance d'entreprise, seules les dispositions minimales selon le Code des obligations doivent être respectées (art. 959*c* et art. 961 ss CO).

Afin de renforcer l'efficacité de la gouvernance d'entreprise, la FINMA estime qu'il est nécessaire de rendre accessible aux parties prenantes des informations sur l'organe responsable de la direction supérieure, sur la direction, sur la procédure d'élection de ces deux organes et sur la politique de risque, en complément des dispositions du droit de la société anonyme.

[8] Notamment IAS 1, IFRS 7 et IFRS Practice Statement « Management Commentary »

[9] « Directive concernant Informations relatives à la Corporate Governance » (Directive Corporate Governance, DCG) du 1er septembre 2014.

Les paramètres des profils d'exigences ainsi que la politique en matière de recrutement et de nomination doivent par exemple être présentés concernant la procédure d'élection et de recrutement des membres de l'organe responsable de la direction supérieure et de la direction. La publication de l'orientation stratégique en matière de risques, du profil de risque et de l'appréciation des risques par la direction doit permettre une évaluation rapide de la situation en matière de risques spécifiques à l'activité. Aucun format spécifique (par exemple tableaux) n'est prescrit pour cet aspect de la publication. Les informations sur les risques doivent compléter la publication selon la Circ.-FINMA 16/1 et compléter la vision globale de la gouvernance des risques de l'établissement.

La plupart des établissements satisfont déjà aux nouvelles exigences en matière de publication, que ce soit volontairement ou en vertu d'autres prescriptions réglementaires.

Dans le cas des banques des catégories de surveillance 1 à 3, les exigences minimales en matière de publication doivent être complétées par des informations qui n'intéressent pas uniquement les actionnaires selon la directive de SIX. Celles-ci incluent notamment des informations sur la structure du groupe financier (s'il existe), sur les autres activités et groupements d'intérêts des membres de l'organe responsable de la direction supérieure et de la direction, sur l'organisation de l'organe responsable de la direction supérieure, sur le système d'indemnisation de l'organe responsable de la direction supérieure et de la direction, sur l'organe de révision et la société d'audit ainsi que sur la politique d'information de l'entreprise.

Environ la moitié des banques des catégories de surveillance 1 à 3 sont cotées et satisfont donc déjà à cette exigence de publication. Les établissements non cotés publient fréquemment sur une base volontaire un grand nombre des informations exigées. La nécessité d'adapter la procédure de publication n'est toutefois pas exclue pour certains établissements, ce qui pourra ponctuellement entraîner des surcoûts.

Afin de limiter la charge que représentent les exigences supplémentaires en matière de publication, il doit être possible de renoncer à une publication séparée, si les informations sont déjà publiées dans le rapport de gestion ordinaire ou sur la base de la Circ.-FINMA 16/1 « Publication – banques ».

3.9 Dispositions transitoires

La plupart des dispositions remaniées n'incluent aucune nouveauté matérielle, mais explicitent et précisent la pratique déjà en vigueur en matière de surveillance. Quelques rares dispositions se traduisent toutefois par des nouveautés et peuvent nécessiter un besoin d'adaptation dans différents établissements. Il s'agit notamment des règles condensées concernant l'indépendance et le système de comités au niveau de la direction supérieure, de l'introduction d'un concept-cadre à l'échelle de l'établissement ainsi que de l'institution et du positionnement approprié de la fonction de CRO au sein de l'établissement. Un délai de transition approprié d'un an à compter de l'entrée en vigueur des présentes modifications est accordé aux établissements concernés afin de concrétiser ces prescriptions. La FINMA peut prolonger ce délai au cas par cas en réponse à une demande motivée.

4 Explications relatives à la révision partielle de la Circ.-FINMA 08/21 « Risques opérationnels – banques »

La révision partielle de la Circ.-FINMA 08/21 prévoit d'une part de simplifier les principes qui doivent désormais s'appliquer à toutes les catégories de risques dans la Circ.-FINMA « Gouvernance d'entreprise – banques » remaniée et d'autre part d'intégrer de nouveaux principes concernant les risques informatiques et les cyberrisques ainsi que le maintien des prestations critiques en cas d'insolvabilité et les risques dans les activités financières transfrontières. Ces adaptations concernent principalement le chapitre IV. Exigences qualitatives concernant la gestion des risques opérationnels.

Tous les passages modifiés dans la Circ.-FINMA 08/21 ont été surlignés en jaune pour l'audition.

4.1 Principe de proportionnalité au chapitre IV. Exigences qualitatives concernant la gestion des risques opérationnels

Le principe de proportionnalité appliqué au chapitre IV a été adapté en ce sens que les petites banques se définissent en principe au travers des catégories de surveillance 4 et 5 de la FINMA. La FINMA peut ordonner des allègements ou des durcissements au cas par cas. Ce n'est plus la banque elle-même ou la société d'audit correspondante qui détermine si une banque est considérée comme une petite ou une grande banque dans le sens de la mise en œuvre des exigences qualitatives du chapitre IV, mais la FINMA au cas par cas.

4.2 Simplification du chapitre IV. Exigences qualitatives concernant la gestion des risques opérationnels

La simplification de la Circ.-FINMA 08/21 concerne d'une part le principe 1 sur les responsabilités de l'organe responsable de la direction supérieure et de la direction et d'autre part le principe 2 sur le concept-cadre et le système de contrôle. Ces principes ont été intégrés dans la Circ.-FINMA « Gouvernance d'entreprise – banques » et s'appliquent désormais à toutes les catégories de risques. Dans l'optique du principe 1 relatif aux responsabilités, l'appétence au risque en matière de risques opérationnels doit continuer à être définie sur la base d'une appréciation séparée de la propension au risque et de la tolérance au risque (classification des risques opérationnels). Cela doit également être pris en considération pour l'élaboration du concept-cadre et en ce qui concerne le principe 2. La classification s'effectue typiquement à l'aide d'une matrice des risques qui inclut pour chaque catégorie[10] de risques opérationnels une évaluation de la probabilité de survenance et de l'étendue des dommages, tant au niveau de la propension au risque que de la tolérance au risque. La classification des différentes catégories de risques opérationnels se fonde notamment sur les évaluations des risques et des contrôles ainsi que sur les résultats de la révision. D'autres instruments et méthodes tels que la collecte et l'analyse de données de pertes ou la réalisation d'analyses de scénarios pour la classification des catégories de risques opérationnels peuvent être utilisés.

[10] Par exemple risques informatiques/cyberrisques, droit/*compliance*, fraude interne, etc.

4.3 Intégration de principes concernant les risques informatiques et les cyberrisques

L'intégration de principes concernant les risques informatiques et les cyberrisques s'effectue par le biais d'une extension du principe 5 existant relatif à l'infrastructure technologique. Des dispositions relatives à l'introduction d'un concept devant inclure des aspects minimaux sont alors prévues tant dans la perspective des risques informatiques que des cyberrisques.

Les exigences minimales à l'égard du concept relatif aux risques informatiques comprennent notamment une vue d'ensemble aussi récente et complète que possible concernant l'environnement réseau informatique. L'établissement et la tenue d'une telle vue d'ensemble doit toutefois être assuré en tenant compte d'une certaine importance pour l'activité, notamment dans le cas des grandes banques. L'aperçu de l'environnement réseau informatique doit notamment servir de base à la gestion des cyberrisques afin d'identifier des points d'attaque potentiels pour des cyberattaques et les points faibles éventuels.

Le concept relatif aux cyberrisques inclut des exigences minimales censées garantir une approche si possible globale de la gestion des cyberrisques, c.-à-d. de la prise en compte des cyberrisques lors de la définition de l'appétence au risque concernant les risques opérationnels jusqu'à un rétablissement rapide de l'activité normale suite à une cyberattaque.

L'identification et la protection des données sensibles et des systèmes contre les cyberattaques sont particulièrement importantes. L'intégrité et la confidentialité des données d'identification des clients doivent notamment être assurées en ce qui concerne les données sensibles. Quant aux systèmes, il s'agit plus particulièrement de protéger contre les cyberattaques ceux qui sont indispensables pour une disponibilité permanente des processus commerciaux critiques pour l'établissement correspondant, mais aussi ceux qui sont en relation avec les fonctions et prestations critiques[11] selon la Circ.-FINMA 08/21, principe 5.

La direction doit par ailleurs garantir l'exécution régulière d'une analyse de vulnérabilité et d'un *penetration testing*, afin d'identifier et de corriger les points faibles concernant notamment les données sensibles et les systèmes dans les meilleurs délais. L'analyse peut être réalisée par des unités internes en présence de ressources qualifiées. Si le personnel et les ressources appropriés font cependant défaut en interne, l'analyse de vulnérabilité et le *penetration testing* doivent être délégués à un prestataire externe. La qualification d'un prestataire externe doit être garantie au moyen d'un examen de la diligence *(due diligence)* lors du choix.

4.4 Maintien des prestations critiques en cas d'insolvabilité

L'objectif de ces exigences consiste à éviter que la défaillance ou l'interruption soudaine de fonctions spécifiques à l'établissement n'aient des conséquences sur la stabilité financière ainsi que la restructuration ou la liquidation d'une banque d'importance systémique. Pour maintenir ces fonctions (fonc-

[11] Cf. chapitre 4.4 Maintien des prestations critiques en cas d'insolvabilité

tions dites « critiques »), il est nécessaire que les banques d'importance systémique s'assurent que les prestations nécessaires aux fonctions critiques (prestations dites « critiques ») puissent être maintenues en présence d'un cas (ou d'un risque) d'insolvabilité. Si les prestations critiques sont fournies par la banque réglementée elle-même (prestations dites *« inhouse »*), les exigences requises pour le maintien en cas d'insolvabilité sont réglées dans la Circ.-FINMA 08/21. Les exigences afférentes à l'acquisition de prestations critiques auprès d'un prestataire tiers ou d'une société de services interne au groupe sont intégrées dans le cadre de la révision partielle de la Circ.-FINMA 08/7 « Outsourcing – banques ».

Les nouvelles prescriptions ont été définies en référence à l'évolution du droit international dans ce domaine et plus particulièrement en tenant compte du document de consultation du CSF « Guidance on Arrangements to Support Operational Continuity in Resolution »[12], qui contient des principes visant à améliorer le maintien des prestations critiques en cas d'insolvabilité. Outre les règles contraignantes pour les banques d'importance systémique, certaines prescriptions sont également applicables aux banques d'importance non systémique, pour autant que cela soit pertinent. Ainsi, même les banques d'importance non systémique doivent établir un inventaire des prestations qui leur semblent les plus importantes. La liquidation ou la restructuration en cas d'insolvabilité doivent ainsi être considérablement simplifiées.

4.5 Risques dans les activités financières transfrontières

La violation du droit étranger peut enfreindre certaines règles suisses en matière de surveillance formulées de manière ouverte, notamment l'exigence de garantie d'une activité irréprochable. Les exigences relatives à la gestion des risques dans les activités transfrontières s'appliquent par ailleurs.

En octobre 2010, la FINMA a décrit, dans un document de position, ses attentes à l'égard de la gestion des risques juridiques et de réputation dans les activités financières transfrontières. Le 19 juillet 2012, elle a publié des réponses aux questions les plus fréquentes (FAQ) dans ce contexte.

Le traitement de ces risques particuliers dans une prise de position distincte était indiqué eu égard aux questions d'interprétation qui se posaient à l'époque. L'environnement juridique et général a évolué entre-temps et les acteurs du marché connaissent et ont conscience des risques dans les activités financières transfrontières.

Grâce à un nouveau principe concernant les risques dans les activités financières transfrontières, les attentes connues de la FINMA sont transférées dans la Circ.-FINMA 08/21 dans l'intérêt d'une consolidation et d'une pérennisation. Le nouveau principe au niveau de la circulaire est formulé sur la base de principes, mais reprend intégralement la pratique administrative décrite dans la prise de position sans en modifier le contenu. Le traitement jusqu'à présent séparé dans un document de position autonome et dans une FAQ est donc désormais inutile.

[12] http://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution.pdf

La FINMA continuera à thématiser la gestion appropriée des risques dans les activités financières transfrontières dans le cadre de la surveillance normale.

4.6 Annexe 3 : Traitement des données électroniques de clients

Suite à l'intégration de la FAQ dans la Circ.-FINMA 08/21, l'annexe 3, dédiée à la gestion des données électroniques de clients, subit également quelques légères adaptations. Certains chiffres marginaux sont ainsi précisés dans les principes 3 (lieu de stockage et accès aux données), 5 (sélection, surveillance et formation des collaborateurs qui ont accès aux CID) et 7 (limitation des risques en relation avec la confidentialité des CID).

5 Explications relatives à la révision partielle de la Circ.-FINMA 10/1 « Systèmes de rémunération »

Le champ d'application obligatoire de la circulaire couvre actuellement les deux principaux groupes d'assurance (Zurich et Swiss Re) ainsi que les banques des catégories de surveillance 1 et 2.

Le Cm 3 indique désormais de façon explicite que la circulaire s'applique en complément de l'ordonnance contre les rémunérations abusives dans les sociétés anonymes cotées en bourse (ORAb). Pour la plupart des établissements, la circulaire garde encore son caractère de ligne directrice. Les différentes exigences sont contraignantes uniquement pour les établissements devant détenir des fonds propres exigibles (exigences minimales selon les art. 7 ss et l'art. 42 OFR) d'au moins 10 milliards de francs. Les établissements de la catégorie de surveillance 2 sont ainsi libérés d'une réglementation infructueuse. La FINMA se réserve toutefois le droit dans des cas justifiés de contraindre les banques ayant des fonds propres minimaux inférieurs à la valeur-seuil à appliquer une partie ou la totalité des dispositions de la circulaire (Cm 9).

Une autre modification concerne la responsabilité du conseil d'administration qui doit désormais approuver chaque année les rémunérations de la direction, des responsables des fonctions de contrôle ainsi que le pool global pour l'établissement financier. Indépendamment de la taille et de la structure de l'établissement financier ou de la complexité de son système de rémunération, le conseil d'administration doit en outre instaurer un comité des rémunérations. Celui-ci doit assurer un soutien indépendant et compétent au conseil d'administration.

D'un point de vue matériel, les systèmes de rémunération devront désormais respecter deux conditions supplémentaires. Premièrement, aucune transaction allant à l'encontre de l'efficacité des éléments du système de rémunération ne doit pouvoir être effectuée (par exemple opérations de couverture). Deuxièmement, les contrats de rémunération doivent être établis de manière à permettre en principe la demande de remboursement des rémunérations variables déjà versées *(« claw-back »)*. Ces deux exigences supplémentaires visent une meilleure efficacité des systèmes de rémunération et devraient pouvoir être appliquées sans trop de difficultés.

6 Conséquences

La nécessité et l'utilité d'une gouvernance d'entreprise appropriée et d'une gestion efficace des risques pour les établissements financiers sont incontestées et ont une nouvelle fois été soulignées par les expériences faites durant la crise des marchés financiers. La sécurité et la stabilité des différents établissements sont améliorées grâce au regroupement de prescriptions modernes concernant la gouvernance d'entreprise et la gestion des risques par les banques dans la nouvelle circulaire. La perspective globale concernant les thèmes de la gouvernance d'entreprise, le système de contrôle interne et la gestion des risques correspond à la pratique actuelle dans le secteur financier. La nouvelle circulaire continue de postuler des exigences fondées sur des principes à l'égard des établissements financiers. La marge de manœuvre pour la mise en œuvre spécifique aux établissements est préservée. Des solutions très variées existent notamment, selon la taille et le profil de risque, en ce qui concerne l'application du modèle *« three lines of defence »* et doivent conserver toute leur légitimité, pour autant que les objectifs fondamentaux en matière de *« checks and balances »* équilibrés et de gestion efficace des risques puissent ainsi être atteints. Une grande partie des nouveautés reflète simplement la pratique en vigueur en matière d'autorisation, mais instaure ainsi plus de clarté et de sécurité juridique. La présente révision ne prévoit aucun changement pour la plupart des banques et négociants en valeurs mobilières assujettis. Pour certains établissements, des efforts ciblés pour satisfaire dorénavant à l'évolution des exigences ne sont cependant pas exclus en ce qui concerne les exigences d'indépendance de l'organe responsable de la direction supérieure, l'obligation d'entretenir un comité des risques séparé pour les banques des catégories de surveillance 1 à 3, la mise en place d'une fonction de CRO distincte, la consolidation du concept-cadre pour la gestion des risques à l'échelle de l'établissement et la mise en œuvre des prescriptions en matière de publication dans le rapport annuel.

L'introduction du principe de proportionnalité dans la nouvelle circulaire marque la poursuite[13] d'une méthode éprouvée pour libérer des établissements des catégories de surveillance 4 et 5 de certaines exigences. Le principe de proportionnalité qui avait été appliqué jusqu'à présent dans la Circ.-FINMA 08/21 est aligné sur celui de la Circ.-FINMA « Gouvernance d'entreprise – banques ». Une trentaine d'établissements sont ainsi considérés comme de petites banques selon la Circ.-FINMA 08/21 et sont libérés de l'obligation de satisfaire à des exigences accrues dans le cadre de cette circulaire.

Dans la Circ.-FINMA 10/1, certains établissements sont exemptés puisque la valeur-seuil des fonds propres minimaux en vue d'une mise en œuvre obligatoire est relevée de 2 milliards de francs à 10 milliards de francs.

[13] Cf. par exemple la Circ.-FINMA 16/1 « Publication – banques ».

7 Suite de la procédure

Les résultats de l'audition seront publiés dans un rapport d'audition. Après d'éventuelles adaptations, la Circ.-FINMA « Gouvernance d'entreprise – banques » et les Circ.-FINMA 08/21 « Risques opérationnels – banques » et 10/1 « Systèmes de rémunération » remaniées devront entrer en vigueur le 1er août 2016.