Autorité bancaire européenne

EBA BS 2011 116 final

27 septembre 2011

Orientations de l'ABE sur la gouvernance interne

(GL 44)

Londres, 27 septembre 2011

Orientations de l'ABE sur la gouvernance interne

Statut de ces orientations

1. Le présent document contient des orientations émises conformément à l'article 16 du règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision n° 2009/78/CE de la Commission (ci-après le «règlement ABE»). Conformément à l'article 16, paragraphe 3, du règlement ABE, les autorités compétentes et les acteurs des marchés financiers doivent tout mettre en œuvre pour respecter ces orientations.

2. Les orientations exposent l'opinion de l'ABE concernant les pratiques de surveillance appropriées au sein du système européen de surveillance financière ou les modalités d'application de la législation de l'Union dans un domaine spécifique. L'ABE escompte donc que toutes les autorités compétentes et tous les acteurs des marchés financiers respectent les orientations qui s'adressent à eux, sauf mention contraire. Les autorités compétentes visées par les orientations sont tenues de s'y conformer en les intégrant dans leurs pratiques de surveillance (en modifiant, par exemple, leur cadre juridique ou leurs règles en matière de surveillance et/ou leurs lignes directrices ou leurs processus de surveillance), y compris lorsque des orientations spécifiques contenues dans le document s'adressent principalement aux établissements.

Exigences de notification

3. Chaque autorité compétente doit indiquer à l'ABE si elle respecte ou entend respecter ces orientations, ou l'informer des raisons pour lesquelles elle n'entend pas les respecter, au plus tard le 28 novembre 2011. La notification devra être adressée par une personne dûment habilitée à informer l'ABE au nom de l'autorité compétente qu'elle représente, à l'adresse électronique: compliance@eba.europa.eu.

4. La notification des autorités compétentes visée au point précédent sera publiée sur le site web de l'ABE, conformément à l'article 16 du règlement ABE.

Des explications complémentaires sur certains aspects spécifiques sont parfois intercalées dans le texte des présentes orientations, pour donner des exemples ou expliciter le raisonnement justifiant une disposition. Le cas échéant, ces explications figurent dans un encadré.

Table des matières

Titre I – Objet, définitions et champ d'application

1. Objet

Les présentes orientations visent à harmoniser les attentes en matière de surveillance et à améliorer la mise en œuvre saine des modalités de la gouvernance interne, conformément à l'article 22 et à l'annexe V de la directive 2006/48/CE et au droit national des sociétés.

2. Champ et niveau d'application

1. Les autorités compétentes requièrent des établissements qu'ils respectent les dispositions énoncées dans ces orientations sur la gouvernance interne.
2. L'application des présentes orientations doit faire l'objet d'un examen par les autorités compétentes dans le cadre du processus de surveillance prudentielle.

Note explicative
Le CECB/l'ABE ont publié des orientations sur le processus de surveillance prudentielle, qui sont disponibles sur le site Internet de l'ABE.

3. Sauf mention contraire, les orientations s'appliquent aux établissements sur une base individuelle, ainsi qu'aux entreprises mères et à leurs filiales sur une base consolidée ou sous-consolidée.
4. Le principe de proportionnalité, tel que défini par les directives 2006/48/CE et 2006/49/CE (telles que modifiées), s'applique à toutes les dispositions visées dans les orientations. Tout établissement a la possibilité de démontrer que l'approche qu'il adopte, eu égard à la nature, à l'échelle ou à la complexité de ses activités, satisfait aux exigences des orientations.

3. Définitions

1. Au sens des présentes orientations, le terme *organe de direction* désigne l'instance dirigeante (ou les instances dirigeantes) de l'établissement regroupant la fonction de surveillance et la fonction exécutive, qui est investie de la plus haute autorité décisionnelle et est habilitée à définir la stratégie, les objectifs et l'orientation générale de l'établissement. L'organe de direction doit inclure les personnes qui dirigent concrètement les activités de l'établissement.
2. Au sens des présentes orientations, le terme *établissement* désigne tout établissement de crédit ou entreprise d'investissement visé par les directives 2006/48/CE et 2006/49/CE.

Titre II – Exigences relatives à la gouvernance interne des établissements

A. Structure et organisation des entreprises

4. Cadre organisationnel

1. L'organe de direction de l'établissement doit s'assurer que ce dernier dispose d'une structure d'entreprise appropriée et transparente. Cette structure doit favoriser et mettre en évidence la gestion efficace et prudente de l'établissement, tant sur une base individuelle qu'au niveau du groupe. Les rapports hiérarchiques et la répartition des responsabilités et de l'autorité au sein de l'établissement doivent être clairs, bien définis, cohérents et appliqués de façon effective.
2. L'organe de direction doit s'assurer que la structure de l'établissement et, le cas échéant, les structures existantes au sein du groupe soient claires et transparentes, tant pour le personnel dudit établissement que pour les autorités chargées de sa surveillance.
3. L'organe de direction doit évaluer la complémentarité et les interactions des différentes composantes de la structure de l'entreprise. La structure ne doit pas réduire la capacité de l'organe de direction à surveiller et à gérer efficacement les risques auxquels l'établissement ou le groupe sont exposés.
4. L'organe de direction doit évaluer dans quelle mesure les changements apportés à la structure du groupe ont une incidence sur sa solidité. L'organe de direction doit procéder sans délai à tout ajustement nécessaire.

> Note explicative
>
> Ces changements peuvent résulter, par exemple, de la mise en place de nouvelles filiales, de fusions ou d'acquisitions, de la vente ou de la liquidation de composantes du groupe ou encore d'événements externes.

5. Contre-pouvoirs dans une structure de groupe

1. Dans une structure de groupe, l'organe de direction de l'entreprise mère de l'établissement doit assumer la responsabilité globale d'une gouvernance interne appropriée pour l'ensemble du groupe, et s'assurer de l'existence d'un cadre de gouvernance adapté à la structure et aux activités du groupe et des entités qui le composent, ainsi qu'aux risques auxquels ils sont exposés.
2. L'organe de direction d'une filiale réglementée d'un groupe doit respecter, au niveau de l'entité, les mêmes valeurs et les mêmes politiques en matière de gouvernance interne que son entreprise mère, à moins que des exigences légales ou de surveillance ou des motifs liés à la proportionnalité n'en disposent autrement. En conséquence, l'organe de direction d'une filiale réglementée doit, dans le cadre de ses propres responsabilités en matière de gouvernance interne, définir ses politiques et évaluer toute décision ou pratique au niveau du

groupe pour vérifier que celles-ci ne placent pas la filiale réglementée en situation d'infraction par rapport aux dispositions légales ou réglementaires ou aux règles prudentielles applicables. L'organe de direction de la filiale réglementée doit également s'assurer que lesdites décisions ou pratiques ne portent pas préjudice:

a. à la gestion saine et prudente de la filiale;

b. à la santé financière de la filiale; ou

c. aux intérêts juridiques des parties intéressées de la filiale.

3. Les organes de direction de l'entreprise mère et de ses filiales doivent appliquer et prendre en considération les dispositions ci-après, en tenant compte des effets de la taille du groupe sur leur gouvernance interne.
4. Lorsqu'il s'acquitte de ses responsabilités en matière de gouvernance interne, l'organe de direction de l'entreprise mère de l'établissement doit garder à l'esprit l'ensemble des problèmes et des risques significatifs susceptibles d'avoir des répercussions sur le groupe, l'entreprise mère elle-même et ses filiales. Il doit donc superviser ses filiales de manière appropriée, dans le respect des dispositions légales et des responsabilités propres en matière de gouvernance aux organes de direction des filiales réglementées.
5. Afin de remplir ses missions en matière de gouvernance interne, l'organe de direction de l'entreprise mère de l'établissement doit:

a. établir une structure de gouvernance qui contribue à une supervision efficace de ses filiales et qui tienne compte de la nature, de l'échelle et de la complexité des différents risques auxquels le groupe et ses filiales sont exposés;

b. adopter, au niveau du groupe, une politique en matière de gouvernance interne à l'intention des filiales, comprenant l'engagement de respecter l'ensemble des exigences applicables dans le domaine de la gouvernance;

c. s'assurer que chaque filiale dispose de ressources suffisantes pour satisfaire tant les normes du groupe que les normes locales en matière de gouvernance;

d. disposer de moyens appropriés pour contrôler le respect par chaque filiale de l'ensemble des exigences applicables dans le domaine de la gouvernance interne; et

e. s'assurer de la clarté et de la transparence des lignes de reporting au sein du groupe, en particulier lorsque les branches d'activité ne coïncident pas avec la structure juridique du groupe.

6. En vue d'assurer la solidité de la gouvernance, une filiale réglementée doit également envisager d'intégrer un nombre suffisant de membres indépendants au sein de son organe de direction. Les membres indépendants de l'organe de

direction sont des directeurs non exécutifs qui ne dépendent ni de la filiale, ni de son groupe, ni de l'actionnaire qui exerce le contrôle.

6. Connaissance de sa propre structure

1. L'organe de direction doit connaître et comprendre pleinement la structure opérationnelle de l'établissement (principe de «*connaissance de sa propre structure*»), et s'assurer de sa compatibilité avec la stratégie économique et le profil de risque qui ont été adoptés.

Note explicative
Il est essentiel que l'organe de direction connaisse et comprenne pleinement la structure opérationnelle de l'établissement. Lorsqu'un établissement crée de nombreuses entités au sein de son groupe, leur nombre, et surtout leurs interconnexions et les transactions exécutées entre elles, peuvent poser des difficultés pour la conception du dispositif de gouvernance interne de l'établissement et pour la gestion et la surveillance des risques du groupe dans son ensemble, ce qui représente en soi un risque.

2. L'organe de direction doit guider et comprendre la structure de l'établissement, son évolution et ses limites, et s'assurer qu'elle reste justifiée et ne présente pas une complexité excessive ou inappropriée. Il est également responsable de l'adoption de stratégies et de politiques saines pour la mise en place de nouvelles structures. De même, l'organe de direction doit reconnaître les risques que pose en soi la complexité de la structure d'une entité et s'assurer que l'établissement est en mesure de fournir des informations en temps utile sur la nature, les statuts, la structure de l'actionnariat et les activités de chaque entité.
3. L'organe de direction de l'entreprise mère de l'établissement doit non seulement comprendre l'organisation des activités du groupe, mais également la raison d'être de ses différentes entités, leurs liens et leurs relations. Ceci inclut la compréhension des risques opérationnels spécifiques au groupe, les expositions intra-groupe, et la manière dont les modes de financement, les fonds propres et les profils de risque du groupe pourraient être affectés, tant dans des circonstances normales que dans un contexte défavorable.
4. L'organe de direction de l'entreprise mère de l'établissement doit s'assurer que les différentes entités du groupe (y compris l'établissement lui-même) reçoivent suffisamment d'informations pour permettre à toutes de percevoir clairement les objectifs généraux du groupe et les risques auxquels celui-ci est exposé. Sur demande, tout échange significatif d'informations entre des entités concernant le fonctionnement opérationnel du groupe doit pouvoir être documenté et rendu accessible sans délai à l'organe de direction, aux fonctions de contrôle et aux autorités de surveillance, le cas échéant.

5. L'organe de direction de l'entreprise mère de l'établissement doit s'assurer qu'il reste en permanence informé des risques inhérents à la structure du groupe. Ces éléments peuvent inclure:
   a. des informations sur les principaux facteurs de risque;
   b. des rapports d'évaluation réguliers sur la structure globale de l'établissement et sur la conformité des activités des différentes entités avec la stratégie adoptée.

7. Activités non conventionnelles ou non transparentes

1. Lorsqu'un établissement exerce une activité dans le cadre de structures ad hoc ou de structures liées, ou bien dans des juridictions faisant obstacle à la transparence ou ne respectant pas les normes bancaires internationales, l'organe de direction doit en comprendre les objectifs et la structure, ainsi que les risques spécifiques afférents. L'organe de direction ne doit accepter ces activités que lorsqu'il a acquis la certitude que les risques seront gérés de manière appropriée.

Note explicative

En complément de ce principe, les autorités compétentes peuvent également appliquer les *Principes fondamentaux pour un contrôle bancaire efficace* élaborés par le Comité de Bâle sur le contrôle bancaire, lorsqu'elles évaluent des activités exercées dans des territoires qui ne respectent pas pleinement le principe de transparence ou qui ne satisfont pas aux normes bancaires internationales.

L'établissement peut avoir des raisons légitimes d'exercer une activité dans certains territoires (ou avec des entités ou des homologues exerçant leurs activités dans ces territoires) ou de mettre en place des structures particulières (par exemple, des structures ad hoc ou des fiducies d'entreprise). Néanmoins, l'exercice d'activités dans des territoires qui ne respectent pas pleinement le principe de transparence ou qui ne satisfont pas aux normes bancaires internationales (par exemple, dans le domaine de la surveillance prudentielle, de la fiscalité, de la lutte contre le blanchiment de capitaux ou le financement du terrorisme), ou par l'intermédiaire de structures complexes ou non transparentes, peut comporter des risques spécifiques sur les plans juridique et financier, comme sur celui de la réputation. Cette situation peut également nuire à la capacité de l'organe de direction à surveiller ces activités de manière appropriée, et entraver la réalisation d'un contrôle bancaire efficace. Ces dispositifs ne doivent donc être approuvés et maintenus que lorsque leur objectif a été défini et compris, qu'une surveillance efficace est assurée et que tous les risques substantiels potentiellement posés par ces structures peuvent être gérés de manière appropriée.

Par conséquent, l'organe de direction doit accorder une attention toute particulière à ces situations, dans la mesure où elles rendent très difficile la compréhension de la structure du groupe.

2. L'organe de direction doit en permanence définir, appliquer et réviser des stratégies, des politiques et des procédures appropriées régissant l'approbation et le maintien de ces structures et activités, afin de s'assurer qu'elles restent cohérentes par rapport à leur objectif initial.

3. L'organe de direction doit s'assurer que des mesures appropriées sont prises pour prévenir ou atténuer les risques liés à ces activités, et notamment que:

   a. l'établissement dispose de politiques, de procédures et de processus documentés adéquats (par exemple, limites applicables, exigences en matière d'information) régissant l'examen, l'approbation et la gestion des risques liés à ces activités, en tenant compte des conséquences pour la structure opérationnelle du groupe;

   b. les informations relatives à ces risques et activités sont accessibles à la direction et aux auditeurs de l'établissement et sont transmises à l'organe de direction et aux autorités de surveillance;

   c. l'établissement évalue périodiquement s'il y a lieu de poursuivre l'exercice des activités qui nuisent à la transparence.

4. Les mêmes mesures doivent être prises lorsqu'un établissement exerce des activités non conventionnelles ou non transparentes pour le compte de ses clients.

Note explicative

Les activités non conventionnelles ou non transparentes exercées pour le compte de clients (par exemple, pour aider des clients à établir des structures dans des juridictions extraterritoriales, mettre au point des structures complexes et financer des transactions pour leur compte ou fournir des services de fiducie) posent des défis similaires en matière de gouvernance interne et peuvent engendrer des risques significatifs, tant sur le plan opérationnel que sur celui de la réputation. C'est pourquoi les mêmes mesures de gestion des risques doivent être prises que lorsqu'il s'agit d'activités exercées pour le compte propre de l'établissement.

5. Toutes ces structures et ces activités doivent faire l'objet d'audits internes et externes réguliers.

B. Organe de direction

B.1 Obligations et responsabilités de l'organe de direction

8. Responsabilités de l'organe de direction

1. L'organe de direction doit détenir la responsabilité globale de l'établissement et en définir la stratégie. Les responsabilités de l'organe de direction doivent être clairement définies dans un document écrit et être approuvées.

Note explicative
La bonne exécution des responsabilités de l'organe de direction est à la base d'une gestion saine et prudente de l'établissement. Les responsabilités fixées par écrit doivent également être conformes au droit des sociétés national.

2. Les principales responsabilités de l'organe de direction doivent inclure la détermination et la surveillance des éléments suivants:

   a. la stratégie économique globale de l'établissement au sein du cadre légal et réglementaire applicable, en tenant compte de la solvabilité et des intérêts financiers à long terme de l'établissement;

   b. la politique et la stratégie globales de l'établissement en matière de risque, y compris en termes de tolérance/appétit au risque et son cadre de gestion des risques;

   c. les montants, la nature et la répartition des capitaux internes et des fonds propres suffisants pour couvrir les risques auxquels l'établissement est exposé;

   d. une structure organisationnelle solide et transparente, dotée de canaux de communication et de notification efficaces;

   e. une politique concernant la nomination et la succession des personnes physiques aux postes clés de l'établissement;

   f. un cadre de rémunération conforme aux stratégies de l'établissement en matière de risques;

   g. les principes de gouvernance et les valeurs d'entreprise de l'établissement, comprenant notamment un code de conduite ou un document comparable; et

   h. un cadre de contrôle interne adéquat et efficace, comprenant des fonctions efficaces de contrôle des risques, de vérification de la conformité et d'audit interne, ainsi qu'un cadre approprié de comptabilité et d'information financière.

3. L'organe de direction doit également réexaminer et ajuster régulièrement ces politiques et stratégies. Il est chargé d’assurer une communication appropriée avec les autorités de surveillance et les autres parties intéressées.

9. Évaluation du cadre de gouvernance interne

1. L'organe de direction doit contrôler et évaluer périodiquement l'efficacité du cadre de gouvernance interne de l'établissement.
2. Un examen du cadre de gouvernance interne et de sa mise en œuvre doit être réalisé au moins une fois par an. Cet examen doit être axé sur les éventuels changements intervenus dans les facteurs internes et externes ayant une incidence sur l'établissement.

10. Fonctions exécutives et de surveillance de l'organe de direction

1. Les fonctions exécutives et de surveillance de l'organe de direction de l'établissement doivent interagir efficacement.

Note explicative

Les États membres utilisent généralement l'une ou l'autre de ces **structures de gouvernance**: une structure moniste ou une structure dualiste. Dans les deux cas, l'organe de direction joue toujours deux rôles distincts dans l'administration de l'établissement: l'un dans le cadre de sa fonction exécutive et l'autre dans celui de sa fonction de surveillance, que ce soit directement ou par l'intermédiaire de comités.

La fonction exécutive formule des propositions quant à l'orientation de l'établissement; elle garantit la mise en œuvre efficace de la stratégie et assume la responsabilité du fonctionnement courant de l'établissement.

La fonction de surveillance supervise et conseille la fonction exécutive. Son rôle de supervision consiste à émettre des critiques constructives lors de la mise au point de la stratégie de l'établissement, à contrôler la performance de la fonction exécutive et la réalisation des objectifs convenus, ainsi qu'à garantir l'intégrité de l'information financière et l'efficacité de la gestion des risques et des contrôles internes.

En vue d'assurer une bonne gouvernance, les fonctions exécutive et de surveillance de l'établissement doivent interagir efficacement pour mettre en œuvre la stratégie adoptée, et notamment pour gérer les risques auxquels l'établissement est exposé. S'il peut exister des différences significatives entre les cadres législatifs et réglementaires des différents pays, ces divergences ne peuvent pas nuire à la bonne interaction de ces deux fonctions, que l'organe de direction soit composé d'une seule entité ou de plusieurs.

2. Dans le cadre de sa fonction de surveillance, l'organe de direction doit:

    a. être en situation et en mesure de contester et de critiquer de manière constructive les propositions, les explications et les informations soumises

par les membres de l'organe de direction dans le cadre de sa fonction exécutive;

b. s'assurer de la mise en œuvre cohérente de la stratégie, du profil de tolérance/appétit au risque et des politiques de l'établissement, ainsi que du maintien de critères de performance compatibles avec la solvabilité et les intérêts financiers à long terme de l'établissement; et

c. contrôler la performance, au regard de ces critères, des membres de l'organe de direction dans le cadre de sa fonction exécutive.

3. Dans le cadre de sa fonction exécutive, l'organe de direction doit coordonner les stratégies de l'établissement sur le plan opérationnel et en matière de risques, en concertation avec l'organe de direction dans le cadre de sa fonction de surveillance, avec lequel il doit également discuter régulièrement de la mise en œuvre de ces stratégies.
4. Chaque fonction doit fournir à l'autre des informations suffisantes. Dans le cadre de sa fonction exécutive, l'organe de direction doit informer régulièrement et de manière exhaustive, et, le cas échéant, sans délai, l'organe de direction dans le cadre de sa fonction de surveillance des éléments nécessaires à l'évaluation d'une situation, à la gestion de l'établissement et au maintien de sa sécurité financière.

B.2 Composition et fonctionnement de l'organe de direction

11. Composition, nomination et succession des membres de l'organe de direction

1. L'organe de direction doit disposer d'un nombre de membres adéquat, et sa composition doit être appropriée. L'organe de direction doit être doté de politiques concernant la sélection, le contrôle et la planification de la succession de ses membres.
2. L'établissement doit fixer la taille et la composition de son organe de direction en tenant compte de la taille et de la complexité de sa structure, ainsi que de la nature et de la portée de ses activités. La sélection des membres de l'organe de direction doit garantir un niveau d'expertise collective suffisant.
3. L'organe de direction doit identifier et sélectionner des candidats qualifiés et expérimentés et garantir une planification appropriée des successions, en tenant dûment compte de toute autre exigence légale en matière de composition, de nomination ou de succession.
4. L'organe de direction doit s'assurer que l'établissement dispose de politiques régissant la sélection de nouveaux membres et la reconduction des membres en exercice. Ces politiques doivent inclure la description des qualifications et des connaissances nécessaires pour garantir une expertise suffisante.
5. Les membres de l'organe de direction doivent être nommés pour une durée appropriée. Les nominations en vue d'une reconduction doivent s'appuyer sur le

profil susmentionné et ne doivent avoir lieu qu'après un examen minutieux de la performance du membre concerné lors de son précédent mandat.

6. Lorsqu'il fixe un plan de succession pour ses membres, l'organe de direction doit tenir compte de la date d'expiration du contrat ou du mandat de chaque membre, afin de prévenir, dans la mesure du possible, le remplacement simultané d'un trop grand nombre de membres.

12. Engagements, indépendance et gestion des conflits d'intérêts au sein de l'organe de direction

1. Les membres de l'organe de direction doivent s'impliquer activement dans le fonctionnement de l'établissement et être en mesure d'émettre des jugements et de prendre des décisions de manière personnelle, judicieuse, objective et indépendante.
2. La sélection des membres de l'organe de direction doit garantir un niveau suffisant d'expertise et d'indépendance en son sein. L'établissement doit s'assurer que les membres de l'organe de direction sont en mesure de consacrer suffisamment de temps et de déployer suffisamment d'efforts pour assumer efficacement leurs responsabilités.
3. Les membres de l'organe de direction ne doivent être engagés que dans un nombre limité de mandats ou autres activités professionnelles qui requièrent beaucoup de temps. En outre, les membres doivent informer l'établissement de leurs activités professionnelles secondaires (par exemple, des mandats pour le compte d'autres entreprises). Le président étant investi d'un plus grand nombre de responsabilités et de missions, il est attendu de ce dernier qu'il y consacre davantage de temps.
4. Le temps minimal que tous les membres de l'organe de direction sont censés consacrer à leur fonction doit être indiqué par écrit. Lorsqu'ils envisagent de nommer un nouveau membre, ou lorsqu'ils sont informés de l'exercice d'un nouveau mandat par l'un d'eux, les membres de l'organe de direction doivent examiner dans quelle mesure ce membre disposera de suffisamment de temps pour assumer ses responsabilités envers l'établissement. L'assiduité des membres de l'organe de direction dans le cadre de sa fonction de surveillance doit être rendue publique. L'établissement doit également envisager de divulguer l'absence prolongée de membres de l'organe de direction dans le cadre de sa fonction exécutive
5. Les membres de l'organe exécutif doivent être en mesure d'agir de manière objective, critique et indépendante. Les mesures visant à renforcer leur capacité à exercer un jugement objectif et indépendant doivent notamment inclure la sélection de membres à partir d'un échantillon suffisamment large de candidats et la participation d'un nombre suffisamment important de membres non exécutifs.

Note explicative

Si les fonctions exécutive et de surveillance de l'organe de direction sont formellement séparées, l'objectivité et l'indépendance de l'organe de direction dans le cadre de sa fonction de surveillance doivent néanmoins être garanties grâce à une sélection appropriée de membres indépendants.

6. L'organe de direction doit disposer d'un document écrit régissant sa politique en matière de gestion des conflits d'intérêts à l'intention de ses membres. Cette politique doit préciser:

   a. l'obligation faite aux membres d'éviter les conflits d'intérêts qui n'ont pas été communiqués à l'organe de direction et approuvés par celui-ci, et, à défaut, de garantir une bonne gestion de ceux-ci;

   b. une procédure d'examen ou d'approbation à laquelle les membres doivent être soumis avant d'entreprendre certaines activités (par exemple, l'exercice d'une fonction auprès d'un autre organe de direction), afin de garantir que ce nouvel engagement ne crée pas de conflit d'intérêts;

   c. l'obligation faite aux membres d'informer l'établissement de toute situation susceptible de créer un conflit d'intérêts ou ayant déjà abouti à un conflit d'intérêts;

   d. la responsabilité des membres de s'abstenir lors d'une prise de décision ou d'un vote sur tout sujet qui les placerait en situation de conflit d'intérêts ou pour lequel leur objectivité ou leur capacité de remplir correctement leurs obligations envers l'établissement pourraient être compromises de quelqu'autre manière que ce soit;

   e. des procédures adéquates pour que les transactions avec des parties liées s'effectuent sur un pied d'égalité; et

   f. les modalités selon lesquelles l'organe de direction traiterait d'un éventuel manquement à cette politique.

13. Qualifications de l'organe de direction

1. Les membres de l'organe de direction doivent disposer des compétences requises pour occuper leurs postes, et les conserver, y compris au moyen de formations. Ils doivent comprendre clairement les dispositifs de gouvernance de l'établissement et le rôle qu'ils y jouent.
2. Les membres de l'organe de direction doivent posséder, tant individuellement que collectivement, l'expertise, l'expérience, les compétences, la compréhension et les qualités personnelles nécessaires, notamment sur le plan du professionnalisme et de l'intégrité, pour accomplir correctement leurs missions.
3. Les membres de l'organe de direction doivent tenir à jour leur connaissance des activités de l'établissement, à un niveau en adéquation avec leurs

responsabilités. Cette connaissance inclut une compréhension appropriée des domaines dont ils ne sont pas directement responsables mais dont ils ont à répondre collectivement.

4. Collectivement, ils doivent comprendre pleinement la nature de l'activité et des risques y afférents, et doivent posséder une expertise et une expérience adéquats en rapport avec chacune des activités significatives que l'établissement entend entreprendre, afin de garantir une gouvernance et une surveillance efficaces.
5. L'établissement doit disposer d'une procédure solide pour garantir que les membres de l'organe de direction possèdent des qualifications suffisantes, tant sur le plan individuel que collectif.
6. Les membres de l'organe de direction doivent acquérir des connaissances et des compétences pour assumer leurs responsabilités, et les conserver et les approfondir. Les établissements doivent s'assurer que les membres ont accès à des programmes de formation sur mesure, lesquels doivent tenir compte des lacunes constatées dans le profil de connaissances dont l'établissement a besoin, ainsi que des connaissances effectives des membres. Les domaines susceptibles d'être couverts comprennent notamment les outils et les modèles de gestion des risques de l'établissement, les développements nouveaux, les changements apportés à l'organisation, les produits complexes, les nouveaux produits ou encore les marchés et les fusions. La formation doit également porter sur les domaines d'activité dont les membres ne sont pas directement responsables à titre individuel. L'organe de direction doit consacrer suffisamment de temps et de ressources, notamment budgétaires, à la formation.

14. Fonctionnement organisationnel de l'organe de direction

1. L'organe de direction doit définir des pratiques et des procédures appropriées en matière de gouvernance interne pour régir sa propre organisation et son fonctionnement, et disposer des moyens nécessaires pour garantir leur respect et leur réexamen régulier en vue de les améliorer.

Note explicative
Le respect, par l'organe de direction, de pratiques et de procédures saines en matière de gouvernance interne envoie des signaux importants, tant au sein de l'établissement qu'à l'extérieur, concernant les politiques et les objectifs dudit établissement en matière de gouvernance. Les pratiques et les procédures incluent la fréquence, les méthodes de travail et les procès-verbaux des réunions, le rôle du président et la mise en œuvre de comités.

2. L'organe de direction doit se réunir régulièrement afin d'accomplir ses missions de manière adéquate et efficace. Les membres de l'organe de direction doivent consacrer suffisamment de temps à la préparation des réunions. La préparation

inclut notamment l'établissement d'un ordre du jour. Le procès-verbal d'une réunion doit détailler les points inscrits à l'ordre du jour et indiquer clairement les décisions prises et les mesures arrêtées. Ces pratiques et procédures, ainsi que les droits, les responsabilités et les activités clés de l'organe de direction, doivent être consignées par écrit et faire l'objet d'un réexamen périodique par l'organe de direction.

Évaluation du fonctionnement de l'organe de direction

3. L'organe de direction doit évaluer de manière régulière, sur un plan tant individuel que collectif, que ses activités, pratiques et procédures en matière de gouvernance, ainsi que le fonctionnement de ses comités, sont mis en œuvre de manière effective et efficace. Il est possible de recourir à des experts externes pour réaliser cette évaluation.

Rôle du président de l'organe de direction

4. Le président doit s'assurer que les décisions de l'organe de direction sont prises de manière judicieuse et éclairée. Il doit encourager et favoriser des discussions ouvertes et critiques et s'assurer que les opinions divergentes peuvent être exprimées et débattues dans le cadre du processus de prise de décisions.

> Note explicative
>
> Le président de l'organe de direction joue un rôle essentiel dans son bon fonctionnement. Il détermine la direction et assume la responsabilité de l'efficacité du fonctionnement global de l'organe de direction.

5. Dans un système moniste, le poste de président de l'organe de direction et celui de directeur général de l'établissement ne peuvent pas être occupés par la même personne. Lorsque le président de l'organe de direction est également le directeur général de l'établissement, ledit établissement doit mettre en place des mesures visant à réduire autant que possible l'affaiblissement potentiel de ses contre-pouvoirs.

> Note explicative
>
> Les dispositifs de contre-pouvoirs peuvent inclure par exemple la nomination d'un membre indépendant et expérimenté au sein de l'organe de direction dans le cadre de sa fonction de surveillance, ou la mise en place d'un poste similaire.

Comités spécialisés de l'organe de direction

6. Dans le cadre de sa fonction de surveillance, l'organe de direction doit envisager, en tenant compte de la taille et de la complexité de l'établissement, de mettre en place des comités spécialisés composés de membres de l'organe de direction (d'autres personnes peuvent y être invitées lorsque leur expertise spécifique ou leurs conseils sont pertinents pour une question donnée). Les

comités spécialisés peuvent inclure un comité d'audit, un comité des risques, un comité de rémunération, un comité de nomination ou des ressources humaines et/ou un comité de gouvernance, d'éthique ou de vérification de la conformité.

Note explicative

La délégation de prérogatives à ces comités ne décharge en aucune manière l'organe de direction de ses missions et responsabilités collectives dans le cadre de sa fonction de surveillance, mais peut l'aider dans certains domaines spécifiques en facilitant la conception et la mise en œuvre de pratiques et de décisions en matière de bonne gouvernance.

7. Un comité spécialisé doit présenter une combinaison optimale d'expertise, de compétences et d'expérience qui lui permettent de comprendre pleinement les questions qui le concernent, de les évaluer de façon objective et de les aborder de manière innovante. Il doit comprendre un nombre suffisant de membres indépendants. Chaque comité doit recevoir un mandat écrit (précisant le champ de ses compétences) de l'organe de direction dans le cadre de sa fonction de surveillance, et doit disposer de procédures de travail établies. La composition et la présidence d'un comité peuvent faire l'objet d'une rotation périodique.

Note explicative

Le renouvellement des membres et de la présidence permet d'éviter les concentrations indues de pouvoir et de favoriser les idées neuves.

8. Les présidents des différents comités doivent régulièrement rendre compte à l'organe de direction. Les comités spécialisés doivent interagir de manière appropriée afin de garantir la cohérence et l'absence de lacune dans leurs travaux. Cette exigence peut prendre la forme d'une participation transversale: le président ou un membre d'un comité spécialisé peut également être membre d'un autre comité spécialisé.

Comité d'audit

9. Un comité d'audit (ou une instance équivalente) doit, entre autres, contrôler l'efficacité des systèmes de contrôle interne, d'audit interne et de gestion des risques de l'entreprise, superviser les auditeurs externes de l'établissement, formuler des recommandations, en vue de leur approbation par l'organe de direction, sur la nomination, la rémunération et la révocation des auditeurs externes, examiner et approuver la portée et la fréquence des audits, examiner les rapports d'audit, et vérifier que l'organe de direction dans le cadre de sa fonction exécutive prend, en temps utile, les mesures correctives nécessaires pour remédier aux faiblesses en matière de contrôle, au non-respect des lois, des réglementations et des politiques, et aux autres problèmes identifiés par les

auditeurs. En outre, le comité d'audit doit superviser la mise en place de politiques comptables par l'établissement.

Note explicative
Voir également l'article 41 de la directive 2006/43/CE concernant les contrôles légaux des comptes annuels et des comptes consolidés.

10. Le président du comité doit être indépendant. Si le président était auparavant membre de la fonction exécutive de l'établissement, un laps de temps approprié doit s'écouler avant qu'il ne prenne ses fonctions en tant que président du comité.
11. Les membres du comité d'audit dans son ensemble doivent posséder une expérience pratique récente et pertinente dans le domaine des marchés financiers, ou avoir acquis, dans le cadre de leurs activités antérieures, une expérience professionnelle suffisante directement liée à l'activité des marchés financiers. Dans tous les cas, le président du comité d'audit doit posséder des connaissances et une expérience spécialisées dans l'application des principes comptables et des procédures de contrôle interne.

Comité des risques

12. Un comité des risques (ou une instance équivalente) doit conseiller l'organe de direction sur la tolérance/appétit au risque, actuelles et à venir, de l'établissement et sur sa stratégie en la matière, ainsi que superviser la mise en œuvre de cette dernière. Pour renforcer son efficacité, le comité des risques doit communiquer régulièrement avec la fonction de contrôle des risques et le directeur des risques de l'établissement, et, le cas échéant, pouvoir recourir à des conseils externes, en particulier en ce qui concerne des propositions de transactions stratégiques, comme les fusions et les acquisitions.

B.3 Cadre de l'exercice des activités

15. Valeurs de l'entreprise et code de conduite

1. L'organe de direction doit définir et favoriser des normes éthiques et professionnelles élevées.

Note explicative
Lorsque la réputation d'un établissement est remise en question, la perte de confiance peut se révéler difficile à combler et peut avoir des répercussions sur l'ensemble du marché. La mise en place de normes appropriées (par exemple, un code de conduite) pour favoriser un comportement professionnel et responsable à tous les échelons de l'établissement devrait contribuer à réduire les risques auxquels ce

dernier est exposé. En particulier, les risques opérationnels et les risques pour la réputation seront moins importants si une priorité élevée est accordée à ces normes et si celles-ci sont mises en œuvre avec diligence.

2. L'organe de direction doit mettre en place des politiques claires concernant la façon dont ces normes sont respectées.
3. La mise en œuvre et le respect de ces normes doivent être revus de manière continue. Les résultats doivent être communiqués régulièrement à l'organe de direction.

16. Conflits d'intérêts au niveau de l'établissement

1. L'organe de direction doit définir, mettre en œuvre et maintenir des politiques efficaces pour identifier les conflits d'intérêts potentiels et avérés. Les conflits d'intérêts qui ont été portés à la connaissance de l'organe de direction et approuvés par celui-ci doivent être gérés de façon appropriée.
2. Une procédure écrite doit spécifier les relations, services, activités ou transactions de l'établissement qui sont susceptibles d'entraîner des conflits d'intérêts, et préciser les modalités selon lesquelles il y a lieu de gérer ces conflits. Cette procédure doit couvrir les relations et les transactions entre les différents clients de l'établissement et entre l'établissement et:
   a. ses clients (dans le cadre de son modèle commercial et/ou des divers services et activités de l'établissement);
   b. ses actionnaires;
   c. les membres de son organe de direction;
   d. son personnel;
   e. ses principaux fournisseurs ou partenaires commerciaux; et
   f. les autres parties liées (par exemple, son entreprise mère ou ses filiales).
3. L'entreprise mère doit équilibrer les intérêts de toutes ses filiales et examiner la manière dont ces intérêts contribuent à l'objectif et aux intérêts communs du groupe dans son ensemble sur le long terme.
4. La politique en matière de conflits d'intérêts doit préciser les mesures devant être adoptées pour prévenir ou gérer les conflits d'intérêts. Ces procédures et mesures peuvent comprendre:
   a. une séparation adéquate des tâches, en confiant par exemple à des personnes différentes les activités en conflit au sein de la chaîne des transactions ou des services, ou en confiant à des personnes différentes les responsabilités en matière de surveillance et de notification pour les activités en conflit;
   b. le cloisonnement de l'information grâce, par exemple, à la séparation physique de certains services; et

c. des mesures visant à empêcher que des personnes exerçant également une activité en-dehors de l'établissement aient une influence inappropriée au sein de l'établissement dans le cadre de ces activités.

17. Procédures d'alerte interne

1. L'organe de direction doit mettre en place des procédures d'alerte interne appropriées pour communiquer les inquiétudes exprimées par le personnel en matière de gouvernance interne.
2. L'établissement doit adopter des procédures d'alerte interne appropriées, pouvant être utilisées par le personnel pour attirer l'attention sur des inquiétudes significatives et légitimes sur des sujets liés à la gouvernance interne. Ces procédures doivent respecter la confidentialité du personnel exprimant ces inquiétudes. Afin d'éviter les conflits d'intérêts, il doit être possible de formuler des inquiétudes de ce type en dehors des voies hiérarchiques traditionnelles (par exemple, par l'intermédiaire de la fonction de vérification de la conformité ou de la fonction d'audit interne, ou par le biais d'une procédure interne de dénonciation des dysfonctionnements). Les procédures d'alerte doivent être mises à la disposition de l'ensemble du personnel de l'établissement. Les informations fournies par le personnel par l'intermédiaire de la procédure d'alerte doivent, le cas échéant, être transmises à l'organe de direction.

Note explicative
Dans certains États membres, outre les procédures d'alerte interne en place au sein de l'établissement, la possibilité peut être donnée au personnel de communiquer des inquiétudes de ce type à l'autorité de surveillance.

B.4 Politiques d'externalisation et de rémunération

18. Externalisation

1. L'organe de direction doit approuver et réexaminer régulièrement la politique d'externalisation de l'établissement.

Note explicative
Les présentes orientations ne portent que sur la politique générale d'externalisation, les questions particulières liées à l'externalisation étant traitées dans les orientations du CECB relatives à l'externalisation, disponibles sur le site Internet de l'ABE. Les établissements sont censés respecter les deux documents d'orientation. En cas de divergence, les orientations du CECB relatives à l'externalisation doivent

prévaloir car elles sont plus spécifiques. Lorsqu'un aspect n'est pas couvert par les orientations du CECB, le principe général des présentes orientations doit s'appliquer.

2. La politique d'externalisation doit tenir compte de l'incidence de cette pratique sur les activités de l'établissement et sur les risques auxquels il est exposé (notamment sur le plan opérationnel et en matière de réputation et de concentration). Cette politique doit inclure les mécanismes de notification et de contrôle qui doivent être mis en œuvre depuis l'entrée en vigueur d'un accord d'externalisation jusqu'à son terme (y compris l'élaboration du dossier d'externalisation, la signature du contrat, l'exécution de ce dernier jusqu'à son expiration, les plans d'urgence et les stratégies de sortie). La politique d'externalisation doit être régulièrement réexaminée et actualisée, et les changements nécessaires apportés en temps utile.
3. L'établissement demeure pleinement responsable de l'ensemble des services et activités qu'il externalise, ainsi que des décisions de gestion qui en résultent. Par conséquent, la politique d'externalisation doit expressément indiquer que cette pratique ne soustrait pas l'établissement à ses obligations réglementaires et à ses responsabilités envers ses clients.
4. Cette politique d'externalisation doit préciser que les mécanismes d'externalisation ne peuvent pas entraver les contrôles sur place ou sur pièces de l'établissement et ne peuvent en aucune manière contrevenir aux restrictions émises par le superviseur sur les services et les activités exercés. Cette politique doit également couvrir la sous-traitance interne (par exemple, par une personne morale distincte appartenant au groupe de l'établissement) et tout cas de figure spécifique à un groupe qu'il y a lieu de prendre en compte.

19. Gouvernance de la politique de rémunération

1. La supervision de la politique de rémunération doit revenir en dernier lieu à l'organe de direction de l'établissement.

Note explicative

Les présentes orientations fixent le cadre *général* applicable à la gouvernance de la politique de rémunération. Les aspects *spécifiques* de la question de la rémunération sont traités dans les orientations du CECB relatives à la rémunération publiées en décembre 2010. Les établissements respecteront les deux documents d'orientation.

2. Dans le cadre de sa fonction de surveillance, l'organe de direction doit préserver, approuver et superviser les principes de la politique générale de rémunération de l'établissement. Les procédures mises en place par l'établissement pour fixer la rémunération doivent être claires, bien documentées et transparentes au niveau interne.

3. Outre la responsabilité générale qui revient à l'organe de direction en ce qui concerne la politique globale de rémunération et son examen, une participation adéquate des fonctions de contrôle est nécessaire. Les membres de l'organe de direction, les membres du comité de rémunération et les autres membres du personnel associés à la définition et à la mise en œuvre de la politique de rémunération doivent posséder une expertise pertinente et être en mesure d'émettre un jugement indépendant sur le caractère approprié de ladite politique, y compris sur ses conséquences pour la gestion des risques.
4. La politique de rémunération doit également viser à prévenir les conflits d'intérêts. Dans le cadre de sa fonction exécutive, l'organe de direction ne peut fixer sa propre rémunération. Afin d'éviter cette pratique, il peut par exemple recourir à un comité de rémunération indépendant. Une unité opérationnelle donnée ne peut être en mesure de fixer la rémunération de ses propres fonctions de contrôle.
5. L'organe de direction doit surveiller l'application de la politique de rémunération, afin de s'assurer que celle-ci sert les objectifs prévus. La mise en œuvre de la politique de rémunération doit également faire l'objet d'un examen centralisé et indépendant.

C. Gestion des risques

20. Culture du risque

1. L'établissement doit mettre en place une culture du risque intégrée et globale, sur la base de la compréhension pleine et entière des risques auxquels il est exposé et de la manière dont ils sont gérés, et en tenant compte de sa tolérance/appétit au risque.

Note explicative
L'activité de l'établissement étant principalement liée à la prise de risques, il est fondamental que les risques soient gérés de manière appropriée. Une culture du risque fiable et cohérente à tous les échelons de l'établissement constitue un élément clé d'une gestion efficace des risques.

2. L'établissement doit mettre en place sa culture du risque à l'aide de politiques, d'exemples, de procédures de communication et de programmes de formation du personnel concernant ses responsabilités en matière de risques.
3. Chaque membre de l'organisation doit être pleinement conscient de ses responsabilités en matière de gestion des risques. La gestion des risques ne peut pas se limiter aux spécialistes du risque ou aux fonctions de contrôle. Les différentes unités opérationnelles, sous la supervision de l'organe de direction, doivent assumer la responsabilité principale de la gestion quotidienne des

risques, en tenant compte de la tolérance/appétit au risque de l'établissement et conformément à ses politiques, procédures et contrôles.

4. L'établissement doit disposer d'un cadre global de gestion des risques qui couvre toutes ses unités opérationnelles et administratives, ainsi que toutes ses unités de contrôle, et qui tient dûment compte de l'importance économique de son exposition aux risques et englobe l'ensemble des risques encourus (par exemple, les risques financiers et non financiers, figurant au bilan ou hors bilan, conditionnels ou contractuels ou non). Son champ d'application ne peut pas se limiter aux risques de crédit, de marché et de liquidité et aux risques opérationnels, mais doit également inclure les risques liés aux concentrations, à la réputation, à la conformité et à la stratégie.
5. Le cadre de gestion des risques doit permettre à l'établissement d'adopter des décisions éclairées. Celles-ci doivent être fondées sur les informations tirées de l'identification, de la mesure ou de l'évaluation et du contrôle des risques. Les risques doivent être évalués selon une approche ascendante et descendante, tout au long de la chaîne de gestion et dans toutes les branches d'activité, en utilisant une terminologie cohérente et des méthodologies compatibles dans l'ensemble de l'établissement et de son groupe.
6. Le cadre de gestion des risques doit faire l'objet d'un examen interne ou externe indépendant, et sa conformité par rapport au profil de tolérance/appétit au risque de l'établissement doit être réévaluée régulièrement, compte-tenu des informations transmises par la fonction de contrôle des risques et, le cas échéant, par le comité des risques. Parmi les facteurs qui doivent être examinés figurent les événements internes et externes, y compris la croissance du bilan et des recettes, le renforcement de la complexité des activités de l'établissement, le profil de risque et la structure opérationnelle, l'expansion géographique, les fusions et les acquisitions ou encore le lancement de nouveaux produits ou de nouvelles branches d'activité.

21. Alignement de la rémunération sur le profil de risque

1. La politique et les pratiques de l'établissement en matière de rémunération doivent être cohérentes par rapport à son profil de risque et favoriser une gestion des risques fiable et efficace.

Note explicative
Les présentes orientations fixent le cadre *général* applicable à l'alignement de la politique de rémunération de l'établissement sur son profil de risque. Les aspects *spécifiques* de la politique de rémunération sont traités dans les orientations du CECB de décembre 2010 relatives à la rémunération. Les établissements respecteront les deux documents d'orientation.

2. La politique générale de l'établissement en matière de rémunération doit correspondre à ses valeurs, à sa stratégie économique, à sa tolérance/appétit au risque, ainsi qu'à ses intérêts à long terme. Elle ne peut pas encourager une prise de risques excessive. Toute rémunération variable garantie ou indemnités de départ qui reviennent à récompenser l'échec ne sont pas compatibles avec une gestion fiable des risques ni avec le principe de la rémunération à la performance, et doivent donc, de manière générale, être proscrites.
3. Pour les membres du personnel dont les activités professionnelles ont une incidence significative sur le profil de risque de l'établissement (par exemple, les membres de l'organe de direction, les instances dirigeantes, les preneurs de risques au sein des unités opérationnelles, le personnel responsable du contrôle interne et tout employé percevant une rémunération du même ordre de grandeur que les instances dirigeantes et les preneurs de risques), la politique de rémunération doit mettre en place des dispositions spécifiques pour garantir que leur rémunération soit compatible avec une gestion saine et efficace des risques.
4. La rémunération des membres du personnel des fonctions de contrôle doit être adéquate et conforme à leurs objectifs et à leur performance, et ne peut être liée à la performance des unités opérationnelles qu'ils contrôlent.
5. Lorsque la rémunération est liée à la performance, celle-ci doit reposer sur une combinaison de la performance individuelle et collective. Pour déterminer la performance individuelle, des facteurs autres que la seule performance financière doivent être pris en considération. La mesure de la performance pour l'attribution de primes doit inclure des ajustements correspondant à tous les types de risques et au coût des fonds propres et des liquidités.
6. Il doit y avoir une relation proportionnelle entre la rémunération de base et les primes. Une prime substantielle ne peut être attribuée sous la forme d'un versement anticipé de liquidités, et doit inclure une composante flexible et différée, ajustée en fonction du risque. La date du versement de la prime doit tenir compte de la performance sous-jacente en matière de risques.

22. Cadre de gestion des risques

1. Le cadre de gestion des risques de l'établissement doit comprendre des politiques, des procédures, des limites et des contrôles lui permettant d'identifier, de mesurer ou d'évaluer, de contrôler, d'atténuer et de déclarer, de manière adéquate, continue et en temps utile, les risques posés par ses activités, tant au niveau des branches d'activité que de l'établissement lui-même.
2. Le cadre de gestion des risques de l'établissement doit fournir une orientation spécifique sur la mise en œuvre de ses stratégies. L'établissement doit fixer et maintenir, le cas échéant, des limites internes cohérentes par rapport à son profil de tolérance/appétit au risque et compatibles avec son fonctionnement sain, sa solidité financière et ses objectifs stratégiques. Le profil de risque de

l'établissement (c'est-à-dire la combinaison de ses expositions avérées et potentielles à des risques) doit être maintenu à l'intérieur de ces limites. Le cadre de gestion des risques doit garantir que tout dépassement de ces limites est communiqué à une instance supérieure et fait l'objet d'un suivi approprié.

3. Lorsqu'il identifie et mesure les risques, l'établissement doit mettre en place des outils prospectifs et rétrospectifs pour compléter le travail sur les expositions courantes. Les outils doivent permettre d'agréger les expositions aux risques dans toutes les branches d'activité et contribuer à identifier les concentrations de risques.
4. Les outils prospectifs (comme les analyses de scénarios et les tests de résistance) doivent permettre de déceler les expositions potentielles à des risques dans toute une série de circonstances défavorables; les outils rétrospectifs doivent contribuer à l'examen du profil de risque courant de l'établissement par rapport à sa tolérance/appétit au risque et au cadre de gestion des risques, fournissant ainsi des données pour procéder à d'éventuels ajustements.

Note explicative
Les orientations sur les tests de résistance sont disponibles sur le site Internet de l'ABE.

5. La responsabilité finale de l'évaluation des risques revient uniquement à l'établissement, qui, en conséquence, doit évaluer de manière critique les risques auxquels il est exposé et ne pas s'appuyer exclusivement sur des évaluations externes.

Note explicative
Par exemple, l'établissement doit approuver un modèle de risque qu'il a acheté et l'ajuster à son cadre spécifique pour garantir une identification et une analyse du risque précises et exhaustives. Les évaluations externes des risques (y compris les notations de crédit externes ou les modèles de risque acquis de manière externe) peuvent contribuer à donner une estimation plus exhaustive du risque. Les établissements doivent être conscients de la portée de ces évaluations.

6. Les décisions qui déterminent le niveau des risques ne peuvent être fondées uniquement sur des données quantitatives ou sur des résultats de modèles, mais doivent également tenir compte des limites pratiques et conceptuelles des mesures et des modèles au moyen d'une approche qualitative (y compris à l'aide d'expertises et d'analyses critiques). Il convient de prendre explicitement en considération les tendances et les données pertinentes du contexte macroéconomique afin d'identifier leur incidence potentielle sur les expositions

et les portefeuilles. Ces évaluations doivent être formellement intégrées aux décisions concernant des risques significatifs.

Note explicative

L'établissement doit tenir compte du fait que les résultats des évaluations quantitatives prospectives et des tests de résistance sont extrêmement dépendants des limites et des hypothèses des modèles utilisés (y compris la gravité et la durée du choc et les risques sous-jacents). Par exemple, des résultats faisant état d'un rendement très élevé du capital économique peuvent découler d'une faiblesse du modèle (par exemple, l'exclusion de certains risques pertinents), plutôt que d'une stratégie ou d'une exécution efficaces de l'établissement.

7. Des mécanismes de notification réguliers et transparents doivent être établis afin que l'organe de direction et l'ensemble des unités concernées de l'établissement reçoivent en temps utile des rapports précis, concis, compréhensibles et significatifs, et puissent partager des informations pertinentes sur l'identification, la mesure ou l'évaluation et le contrôle des risques. Le cadre de notification doit être bien défini, documenté et approuvé par l'organe de direction.
8. Si un comité des risques a été mis en place, il doit recevoir régulièrement des rapports formels et des communications informelles, le cas échéant, de la fonction de contrôle des risques et du directeur des risques.

Note explicative

Une communication efficace de l'information sur les risques est essentielle pour l'ensemble du processus de gestion des risques: elle facilite les procédures d'examen et de prise de décision et contribue à prévenir les décisions susceptibles d'accroître involontairement les risques. Une notification efficace des risques exige une évaluation et une communication internes correctes de la stratégie en matière de risques et des données pertinentes en la matière (par exemple, expositions et indicateurs de risque clés), tant sur un plan horizontal, dans l'ensemble de l'établissement, qu'en amont et en aval de la chaîne de gestion.

23. Nouveaux produits

1. L'établissement doit disposer d'une politique bien documentée de validation des nouveaux produits (PVNP), approuvée par l'organe de direction, qui traite de l'ouverture de nouveaux marchés, du lancement de nouveaux produits et services, et de l'introduction de changements significatifs dans les offres existantes.

2. La PVNP de l'établissement doit couvrir tous les aspects à prendre en considération avant que la décision ne soit prise de s'engager sur de nouveaux marchés, de commercialiser de nouveaux produits, de lancer un nouveau service ou d'apporter des changements significatifs à des produits ou services existants. La PVNP doit également inclure les définitions de «nouveau produit», de «nouveau marché» et de «nouvelle activité» telles qu'elles doivent être utilisées dans l'organisation et par les fonctions internes associées au processus de prise de décisions.
3. La PVNP doit définir les principales questions à aborder avant qu'une décision ne soit prise. Celles-ci comprennent notamment l'application de la réglementation, les modèles tarifaires, l'incidence sur le profil de risque, l'adéquation des fonds propres et la rentabilité, l'allocation de ressources adéquates au *front office,* au *back office* et au *middle office*, ainsi que la disponibilité d'outils internes adéquats et de connaissances techniques suffisantes pour comprendre et contrôler les risques afférents. La décision de lancer une nouvelle activité doit clairement spécifier la branche d'activité concernée et les personnes qui en sont responsables. Une nouvelle activité ne peut pas être entreprise avant que les ressources adéquates pour comprendre et gérer les risques afférents ne soient disponibles.
4. La fonction de contrôle des risques doit être associée à la validation des nouveaux produits ou des changements significatifs apportés aux produits existants. Sa contribution doit inclure une évaluation complète et objective des risques engendrés par les nouvelles activités selon plusieurs scénarios différents, de toute lacune potentielle dans les cadres de gestion des risques et de contrôle interne de l'établissement, ainsi que de la capacité de l'établissement à gérer efficacement tout nouveau risque. La fonction de contrôle des risques doit également avoir une vue d'ensemble claire du lancement de nouveaux produits (ou des changements significatifs apportés à des produits existants) dans les différents portefeuilles et branches d'activité, et peut exiger que l'introduction de changements dans les offres existantes soient soumise à la procédure formelle de la PVNP.

D. Contrôle interne

24. Cadre de contrôle interne

1. L'établissement doit mettre au point et maintenir un cadre solide et complet de contrôle interne, y compris des fonctions de contrôle spécifiques et indépendantes jouissant des prérogatives adéquates pour accomplir leurs missions.
2. Le cadre de contrôle interne de l'établissement doit garantir des activités efficaces et efficientes, un contrôle adéquat des risques, une conduite prudente des activités, la fiabilité des informations financières et non financières communiquées, tant sur le plan interne qu'externe, et la conformité avec la loi,

la réglementation, les exigences de surveillance et les règles et décisions internes de l'établissement. Le cadre de contrôle interne doit couvrir la totalité de l'organisation, y compris les activités de l'ensemble des unités opérationnelles et administratives et des unités de contrôle. Le cadre de contrôle interne doit être adapté aux activités de l'établissement et comporter des procédures administratives et comptables saines.

3. Dans l'élaboration de son cadre de contrôle interne, l'établissement doit garantir un processus décisionnel clair, transparent et bien documenté et une répartition claire des responsabilités et de l'autorité, afin d'assurer la conformité avec les règles et les décisions internes. Afin de mettre en œuvre un cadre de contrôle interne solide dans tous les secteurs de l'établissement, les unités opérationnelles et administratives doivent être responsables en premier lieu de la définition et du maintien des politiques et des procédures adéquates en matière de contrôle interne.
4. Un cadre de contrôle interne approprié exige également la vérification du respect de ces politiques et procédures par des fonctions de contrôle indépendantes. Ces dernières doivent inclure une fonction de contrôle des risques, une fonction de vérification de la conformité et une fonction d'audit interne.
5. Les fonctions de contrôle doivent être mises en place à un niveau hiérarchique adéquat et être directement responsables devant l'organe de direction. Elles doivent être indépendantes des unités opérationnelles et administratives qu'elles contrôlent et indépendantes les unes des autres sur le plan organisationnel (puisqu'elles remplissent différentes fonctions). Cependant, dans des établissements moins complexes ou de plus petite taille, les missions de la fonction de contrôle des risques et de la fonction de vérification de la conformité peuvent être fusionnées. Les fonctions de contrôle du groupe doivent superviser les fonctions de contrôle des filiales.
6. Pour qu'une fonction de contrôle soit considérée comme indépendante, les conditions suivantes doivent être remplies:

    a. son personnel ne s'acquitte d'aucune tâche relevant du champ d'application des activités que la fonction de contrôle a pour mission de surveiller et de contrôler;

    b. la fonction de contrôle est séparée sur le plan organisationnel des activités qu'elle est chargée de surveiller et de contrôler;

    c. le responsable de la fonction de contrôle est subordonné à une personne qui n'endosse aucune responsabilité dans la gestion des activités que la fonction de contrôle surveille et contrôle. En général, le responsable de la fonction de contrôle doit être directement responsable devant l'organe de direction et tout comité pertinent, et doit régulièrement assister à leurs réunions; et

d. la rémunération du personnel de la fonction de contrôle ne peut pas être liée à la performance des activités que celle-ci surveille et contrôle, et ne peut pas nuire à son objectivité de quelqu'autre manière que ce soit.

7. Les fonctions de contrôle doivent disposer d'un personnel qualifié en nombre suffisant (au niveau tant de l'entreprise mère que des filiales, dans le cas d'un groupe). Le personnel doit toujours être suffisamment qualifié et doit bénéficier de formations appropriées. Il doit également disposer de systèmes de gestion des données et d'assistance, et avoir accès aux informations internes et externes nécessaires pour assumer ses responsabilités.
8. Les fonctions de contrôle doivent régulièrement soumettre des rapports formels à l'organe de direction concernant les principales faiblesses détectées. Ces rapports doivent comprendre un suivi des conclusions formulées précédemment et, pour chaque nouvelle faiblesse majeure identifiée les risques impliqués, une analyse d'incidence et des recommandations. L'organe de direction doit agir sur la base des conclusions des fonctions de contrôle de manière efficace et en temps utile, et exiger des mesures correctives adéquates.

25. Fonction de contrôle des risques (FCR)

1. L'établissement doit mettre en place une fonction de contrôle des risques exhaustive et indépendante.
2. La FCR doit s'assurer que chaque risque auquel l'établissement est exposé est identifié et traité de manière appropriée par les unités concernées au sein de l'établissement, et qu'un aperçu global de tous les risques pertinents est transmis à l'organe de direction. La FCR doit fournir des informations, des analyses et des expertises indépendantes et pertinentes sur les expositions aux risques, et formuler des conseils quant à la cohérence, par rapport à la tolérance/appétit au risque de l'établissement, des propositions et des décisions de l'organe de direction et des unités opérationnelles et administratives en matière de risques. La FCR peut recommander des améliorations à apporter au cadre de gestion des risques, ainsi que des solutions permettant de remédier à des violations des politiques, procédures et limites relatives aux risques.
3. La FCR doit constituer un élément central de l'organisation de l'établissement et être structurée de manière à pouvoir mettre en œuvre des politiques en matière de risques et contrôler le cadre de gestion des risques. Les établissements de grande taille, complexes et sophistiqués peuvent décider de mettre en place une FCR spécifique pour chaque grande branche d'activité. L'établissement doit toutefois disposer d'une FCR centrale (y compris, le cas échéant, d'une FCR du groupe au sein de l'entreprise mère d'un groupe), qui fournira une vue globale de l'ensemble des risques.
4. La FCR doit être indépendante des unités opérationnelles et administratives dont elle contrôle les risques sans en être isolée. Elle doit posséder une connaissance suffisante des techniques et des procédures de gestion des

risques, ainsi que des marchés et des produits. Les interactions entre les fonctions opérationnelles et la FCR doivent permettre la réalisation de l'objectif consistant à ce que l'ensemble du personnel de l'établissement assume la responsabilité de la gestion des risques.

26. Le rôle de la fonction de contrôle des risques

1. La FCR doit participer activement et à un stade précoce à l'élaboration de la stratégie de l'établissement en matière de risques et à l'ensemble des décisions concernant la gestion des risques significatifs. La FCR doit jouer un rôle essentiel pour garantir que l'établissement dispose de processus efficaces de gestion des risques.

Rôle de la FCR vis-à-vis de la stratégie et de la prise de décisions

2. La FCR doit fournir à l'organe de direction toutes les informations pertinentes en matière de risques (par exemple, au moyen d'une analyse technique sur l'exposition aux risques) dont il a besoin pour déterminer le niveau de tolérance/appétit au risque de l'établissement.
3. La FCR doit également évaluer la stratégie en matière de risques, y compris les objectifs proposés par les unités opérationnelles, et conseiller l'organe de direction en amont de la prise de décision. Les objectifs, y compris en ce qui concerne les notations de crédit et le taux de rentabilité des capitaux propres, doivent être plausibles et cohérents.
4. La FCR doit partager la responsabilité de la mise en œuvre de la stratégie et de la politique de l'établissement en matière de risques avec l'ensemble des unités opérationnelles de celui-ci. Si les unités opérationnelles doivent respecter les limites applicables en matière de risques, la FCR a, quant à elle, la responsabilité de s'assurer que les limites sont compatibles avec le niveau global de tolérance/appétit au risque de l'établissement et de contrôler en permanence que l'établissement ne prend pas de risques excessifs.
5. La participation de la FCR aux processus de prise de décisions doit garantir que les questions relatives aux risques sont dûment prises en considération. Cependant, les décisions prises doivent rester de la responsabilité des unités opérationnelles et administratives et, de manière ultime, de l'organe de direction.

Rôle de la FCR vis-à-vis des transactions avec des parties liées

6. La FCR doit s'assurer que les transactions avec des parties liées soient examinées et que les risques – avérés ou potentiels – qu'elles posent pour l'établissement soient identifiés et dûment évalués.

Rôle de la FCR en matière de complexité de la structure juridique

7. La FCR doit s'efforcer d'identifier les risques significatifs liés à la complexité de la structure juridique de l'établissement.

Note explicative

Ces risques peuvent inclure un déficit de transparence dans la gestion, des risques opérationnels causés par des structures de financement complexes et interconnectées, des expositions internes au groupe, ainsi que le risque de contrepartie et de collatéral immobilisé.

Rôle de la FCR en matière de changements significatifs

8. La FCR doit évaluer dans quelle mesure les risques significatifs identifiés pourraient porter préjudice à la capacité de l'établissement ou du groupe à gérer son profil de risque et à déployer des financements et des capitaux dans des conditions normales et défavorables.
9. Avant que des décisions relatives à des changements significatifs ou à des transactions exceptionnelles ne soient prises, la FCR doit être associée à l'évaluation des incidences de ces changements et de ces transactions exceptionnelles sur le risque global auquel l'établissement et le groupe sont exposés.

Note explicative

Les changements substantiels ou les transactions exceptionnelles peuvent inclure les fusions et les acquisitions, la création ou la vente de filiales ou de structures ad hoc, le lancement de nouveaux produits, les changements apportés aux systèmes, au cadre ou aux procédures de gestion des risques, et les changements apportés à l'organisation de l'établissement.

Voir les orientations conjointes de 2008 des comités de niveau 3 des autorités européennes de surveillance financière (CECB, CERVM et CECAPP) relatives à l'évaluation prudentielle des acquisitions et aux augmentations de participation dans le secteur financier, publiées sur le site Internet de l'ABE. La FCR doit participer activement et à un stade précoce à l'identification des risques pertinents (y compris les conséquences potentielles de la mise en œuvre d'une diligence insuffisante pour identifier les risques consécutifs à une fusion) liés aux changements apportés à la structure du groupe (y compris les fusions et les acquisitions) et doit communiquer ses conclusions directement à l'organe de direction.

Rôle de la FCR en matière de mesures et d'évaluations du risque

10. La FCR doit s'assurer que les mesures et les évaluations du risque interne dans un établissement couvrent un éventail approprié de scénarios et sont soient fondées sur des hypothèses suffisamment prudentes en matière de causalités et de corrélations. Ces éléments doivent inclure des avis qualitatifs à l'échelle

de l'entreprise (y compris des expertises sur les liens entre les risques et la rentabilité de l'établissement et l'environnement opérationnel extérieur.

Rôle de la FCR en matière de contrôle

11. La FCR doit s'assurer que tous les risques identifiés peuvent effectivement faire l'objet d'un contrôle par les unités opérationnelles. La FCR doit régulièrement contrôler le profil de risque avéré de l'établissement et le comparer à ses objectifs stratégiques et à son profil de tolérance/appétit au risque pour permettre à l'organe de direction de prendre des décisions dans le cadre de sa fonction exécutive et de les remettre en cause dans le cadre de sa fonction de surveillance.
12. La FCR doit analyser les tendances et repérer les risques nouveaux ou émergents liés à des changements de conditions et de circonstances. Elle doit également réexaminer régulièrement les résultats en matière de risques avérés par rapport à des estimations antérieures (contrôles a posteriori), afin d'évaluer et d'améliorer la précision et l'efficacité du processus de gestion des risques.
13. La FCR du groupe doit contrôler les risques pris par les filiales. Les incohérences par rapport à la stratégie de groupe qui a été approuvée doivent être communiquées à l'organe de direction compétent.

Rôle de la FCR en matière d'expositions non approuvées

14. La FCR doit être associée de manière adéquate à tout changement apporté à la stratégie de l'établissement, à son profil de tolérance/appétit au risque validé et aux limites applicables.
15. La FCR doit évaluer de manière indépendante toute infraction ou violation (y compris son origine, et en effectuant une analyse juridique et économique du coût réel de la suppression, de la réduction ou de la couverture de l'exposition par rapport au coût potentiel de son maintien). La FCR doit informer, le cas échéant, les unités opérationnelles concernées et formuler des recommandations concernant d'éventuelles mesures correctives.

Note explicative

Les infractions ou les violations par rapport aux stratégies, à la tolérance/appétit au risque ou aux limites en la matière peuvent être causées par de nouvelles transactions, des changements dans l'environnement du marché ou une évolution de la stratégie, des politiques ou des procédures de l'établissement, lorsque les limites ou la tolérance/appétit au risque ne sont pas modifiées en conséquence.

16. La FCR doit jouer un rôle essentiel pour garantir qu'une décision est prise au niveau approprié pour faire suite à une recommandation qu'elle a formulée, qu'elle est appliquée par les unités opérationnelles concernées et qu'elle est

dûment notifiée à l'organe de direction, au comité des risques et à l'unité opérationnelle ou administrative concernée.

17. L'établissement doit prendre les mesures appropriées pour prévenir les comportements frauduleux, sur le plan tant interne qu'externe, ainsi que les manquements à la discipline (par exemple, une infraction aux procédures internes ou un dépassement des limites).

Note explicative
Au sens des présentes orientations, le terme «fraude» inclut les fraudes internes et externes telles que définies dans la directive 2006/48/CE, annexe X, partie 5. Ces éléments incluent les pertes liées à des actes visant à commettre une fraude ou un détournement d'actif ou à enfreindre/contourner une réglementation, une loi ou des règles de l'entreprise, à l'exclusion des cas de discrimination ou d'inapplication des règles en matière de diversité, et impliquant au moins un membre de l'entreprise (fraude interne) et les pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre/contourner la loi (fraude externe).

27. Directeur des risques

1. L'établissement doit nommer une personne au poste de directeur des risques (CRO) pour assumer la responsabilité exclusive de la FCR et pour contrôler le cadre de gestion des risques de l'établissement dans l'ensemble de l'organisation.
2. Le CRO (ou un poste équivalent) doit être responsable de la fourniture d'informations complètes et compréhensibles sur les risques, permettant à l'organe de direction de comprendre le profil de risque global de l'établissement. La même disposition s'applique au CRO de l'établissement mère à l'égard de l'ensemble du groupe.
3. Le CRO doit disposer de suffisamment de savoir-faire, d'expérience pratique, d'indépendance et d'ancienneté pour remettre en question les décisions affectant l'exposition de l'établissement aux risques. L'établissement doit envisager d'accorder un droit de veto au CRO. Le CRO et l'organe de direction ou les comités compétents doivent être en mesure de communiquer directement entre eux sur les questions essentielles liées au risque, y compris sur les situations potentiellement incompatibles avec la tolérance/appétit au risque de l'établissement et sa stratégie en la matière.
4. Si l'établissement souhaite accorder au CRO un droit de veto sur certaines décisions, ses politiques en matière de risques doivent exposer les circonstances dans lesquelles le CRO est habilité à agir de la sorte, ainsi que la nature des propositions concernées (par exemple, une décision de crédit ou d'investissement ou la fixation d'une limite). Les politiques doivent spécifier les

procédures d'intervention par paliers et les procédures de recours, ainsi que les modalités selon lesquelles l'organe de direction est informé.

5. Lorsque les caractéristiques de l'établissement – en particulier sa taille, son organisation et la nature de ses activités – ne justifient pas de confier une telle responsabilité à une personne nommée spécifiquement à cet effet, la fonction peut être remplie par une autre personne expérimentée au sein de l'établissement, dans la mesure où cela n'entraîne pas de conflit d'intérêts.
6. L'établissement doit disposer de procédures documentées pour pourvoir le poste de CRO et pour décharger celui-ci de ses responsabilités. En cas de remplacement du CRO, ce changement nécessite l'accord préalable de l'organe de direction dans le cadre de sa fonction de surveillance. De manière générale, la révocation et la nomination d'un CRO doivent être divulguées et l'autorité de surveillance doit être informée des motifs de cette décision.

28. Fonction de vérification de la conformité

1. L'établissement doit mettre en place une fonction de vérification de la conformité pour gérer le risque de conformité auquel il est exposé.
2. L'établissement doit approuver et mettre en œuvre une politique de conformité qui doit être communiquée à l'ensemble du personnel.

> Note explicative
>
> Le risque de conformité (défini comme le risque effectif ou potentiel pour les revenus et le capital lié aux violations ou au non-respect de lois, de règles, de réglementations, d'accords, de pratiques prescrites ou de normes éthiques) peut entraîner le paiement d'amendes ou de dommages et/ou l'annulation de contrats, et peut nuire à la réputation de l'établissement.

3. L'établissement doit mettre en place une fonction de vérification de la conformité permanente et efficace et nommer une personne responsable de cette fonction pour l'ensemble de l'établissement et du groupe (le responsable de la conformité ou le directeur de la conformité). Dans les établissements de plus petite taille et moins complexes, cette fonction peut être fusionnée avec la fonction de contrôle des risques ou d'autres fonctions administratives (par exemple, les RH, le service juridique, etc.), ou être assistée par ces dernières.
4. La fonction de vérification de la conformité doit s'assurer du respect de la politique en matière de conformité et transmettre à l'organe de direction et, le cas échéant, à la FCR des informations relatives à la gestion du risque de conformité de l'établissement. Les conclusions de la fonction de vérification de la conformité doivent être prises en considération par l'organe de direction et la FCR dans le cadre du processus de prise de décisions.
5. La fonction de vérification de la conformité doit conseiller l'organe de direction sur les lois, les règles, les réglementations et les normes que l'établissement

doit respecter et évaluer l'incidence potentielle de tout changement apporté au cadre juridique ou réglementaire sur les activités de l'établissement.

6. La fonction de vérification de la conformité doit également vérifier que les nouveaux produits et les nouvelles procédures respectent le cadre juridique en vigueur et toute modification ultérieure connue de la législation, de la réglementation ou des exigences de surveillance.

Note explicative
Une attention toute particulière doit être accordée aux situations dans lesquelles l'établissement fournit pour le compte de clients certains services ou met en place des structures pouvant poser des difficultés particulières dans le domaine de la gouvernance interne et susciter des craintes prudentielles (par exemple, en jouant le rôle d'agent pour la constitution de société ou de partenariat, en fournissant des services fiduciaires ou en mettant en place des transactions financières structurées et complexes pour le compte de clients).

29. Fonction d'audit interne

1. La fonction d'audit interne (ci-après «FAI») doit évaluer si la qualité du cadre de contrôle interne de l'établissement permet de dire que celui-ci est efficace et efficient.
2. La FAI doit disposer d'un libre accès à l'ensemble des informations et des documents pertinents de tous les services opérationnels et de contrôle.
3. La FAI doit évaluer la conformité de l'ensemble des activités et des services de l'établissement (y compris la FCR et la fonction de vérification de la conformité) avec ses politiques et procédures. La FAI ne doit donc pas être fusionnée avec une autre fonction. La FAI doit également évaluer si les politiques et procédures en vigueur demeurent adéquates et sont conformes aux exigences légales et réglementaires.
4. La FAI doit en particulier vérifier l'intégrité des processus garantissant la fiabilité des méthodes, techniques, hypothèses et sources d'information utilisées par l'établissement pour ses modèles internes (par exemple, pour établir des modèles de risque et effectuer des mesures comptables). Elle doit également évaluer la qualité et l'utilisation des outils qualitatifs d'identification et d'évaluation des risques. Cependant, afin de renforcer son indépendance, la FAI ne doit pas être directement associée à la conception ou à la sélection de modèles ou d'autres outils de gestion des risques.
5. L'organe de direction doit encourager les auditeurs internes à respecter les normes professionnelles nationales et internationales. Le travail d'audit interne doit être réalisé conformément à un plan d'audit et à des programmes d'audit détaillés, suivant une approche «fondée sur les risques». Le plan d'audit doit être approuvé par le comité d'audit et/ou l'organe de direction.

Note explicative

Les normes établies par l'Institut des auditeurs internes offrent un exemple des normes professionnelles susmentionnées.

6. La FAI doit communiquer directement à l'organe de direction et/ou (le cas échéant) à son comité d'audit ses conclusions et ses suggestions pour apporter des améliorations significatives aux contrôles internes. Toutes les recommandations en matière d'audit doivent être soumises à une procédure formelle de suivi par le niveau de gestion compétent, afin de garantir qu'elles soient prises en compte et que des informations soient communiquées à ce sujet.

E. Systèmes d'information et continuité des activités

30. Système d'information et communication

1. L'établissement doit disposer de systèmes efficaces et fiables d'information et de communication, couvrant l'ensemble de ses activités significatives.

Note explicative

Des informations peu fiables ou trompeuses, fournies par des systèmes mal conçus et mal contrôlés, peuvent être préjudiciables aux décisions de gestion. C'est pourquoi la mise en place et la maintenance de systèmes d'information et de communication couvrant la totalité des activités de l'établissement est une composante essentielle desdites activités. Le plus souvent, cette information circule à la fois sous forme électronique et non électronique.

Un établissement doit notamment avoir connaissance des exigences en matière d'organisation et de contrôle interne qui sont liées au traitement de l'information sous forme électronique, ainsi que de la nécessité de disposer d'une piste d'audit adéquate. Cette disposition s'applique également si les systèmes informatiques sont externalisés auprès d'un prestataire de services.

2. Les systèmes d'information, y compris ceux qui permettent de stocker et d'exploiter les données sous forme électronique, doivent être sécurisés, contrôlés de manière indépendante et assortis de dispositions d'intervention d'urgence adéquates. Lorsqu'il déploie des systèmes informatiques, l'établissement doit respecter les normes généralement acceptées dans ce domaine.

31. Gestion de la continuité des activités

1. L'établissement doit mettre en place une gestion saine de la continuité de ses activités, afin de garantir sa capacité à fonctionner sans interruption et de limiter ses pertes en cas de perturbation grave de ses activités.

> Note explicative
>
> L'activité de l'établissement repose sur plusieurs ressources essentielles (par exemple, les systèmes informatiques, les systèmes de communication, les bâtiments). L'objectif de la gestion de continuité des activités est de limiter les conséquences opérationnelles, financières et juridiques, le préjudice pour sa réputation, ainsi que les autres effets significatifs engendrés par un sinistre ou une indisponibilité prolongée de ces ressources et par la perturbation des procédures opérationnelles ordinaires de l'établissement qui en résulte. D'autres mesures de gestion des risques peuvent consister à réduire la probabilité de ces incidents ou à transférer leurs conséquences financières à des tiers (par exemple, en souscrivant une assurance).

2. Afin de mettre en place une gestion raisonnable de la continuité de ses activités, un établissement doit analyser avec soin son exposition à des perturbations graves de ses activités et évaluer (sur le plan tant quantitatif que qualitatif) leurs incidences potentielles au moyen d'une analyse interne et/ou externe de données et de scénarios. Cette analyse doit couvrir l'ensemble des unités opérationnelles et administratives, ainsi que la FCR, et tenir compte de leur interdépendance. En outre, une fonction spécifique de continuité d'activité indépendante, la FCR ou la fonction chargée de la gestion du risque opérationnel doit être activement associée à la procédure. Les résultats de l'analyse doivent contribuer à la définition des priorités et des objectifs de l'établissement en matière de reprise des activités.

> Note explicative
>
> En ce qui concerne la fonction chargée de la gestion du risque opérationnel, voir également la directive 2006/48/CE, annexe X, parties 3 et 4, qui requiert une fonction indépendante de ce type pour les établissements appliquant une AMA. Les missions de cette fonction sont décrites dans les orientations (publiées en 2006) relatives à la validation, paragraphes 615 à 620, disponibles sur le site Internet de l'ABE.

3. Sur la base de l'analyse susmentionnée, l'établissement doit mettre en place:

    a. des plans d'intervention et de continuité des activités, qui garantissent que l'établissement réagisse de manière appropriée aux urgences et qu'il soit en mesure de maintenir ses activités les plus importantes en cas de perturbation de ses procédures opérationnelles ordinaires;

b. des plans de recouvrement des ressources essentielles lui permettant de recouvrer ses procédures opérationnelles ordinaires dans un délai approprié. Tout risque résiduel lié à des perturbations potentielles des activités doit être compatible avec la tolérance/appétit au risque de l'établissement.

4. Les plans de gestion de crise, de continuité des activités et de reprise des activités doivent être consignés par écrit et mis en œuvre avec soin. La documentation doit être mise à la disposition des unités opérationnelles et administratives et de la FCR, et doit être stockée dans des systèmes physiquement séparés et aisément accessibles en cas d'incident. Une formation appropriée doit être dispensée. Les plans doivent être régulièrement testés et actualisés. Tout problème ou échec constaté lors des tests doit être documenté et analysé, et les plans doivent être révisés en conséquence.

F. Transparence

32. Responsabilisation

1. Les stratégies et les politiques doivent être communiquées à tout le personnel concerné, dans l'ensemble de l'établissement.
2. Les membres du personnel de l'établissement doivent comprendre et respecter les politiques et procédures liées à leurs missions et responsabilités.
3. En conséquence, l'organe de direction doit informer les membres du personnel concerné des stratégies et des politiques de l'établissement de manière claire et cohérente et maintenir ces informations à jour, au moins au niveau nécessaire pour leur permettre d'accomplir les tâches qui leur incombent. Cette information peut être transmise par l'intermédiaire d'orientations écrites, de manuels ou d'autres supports.

33. Gouvernance interne et transparence

1. Le cadre de gouvernance interne de l'établissement doit être transparent. L'établissement doit présenter sa situation actuelle et ses perspectives pour l'avenir de manière claire, équilibrée, précise et en temps utile.

Note explicative
L'objectif de transparence dans le domaine de la gouvernance interne vise à fournir à l'ensemble des parties prenantes de l'établissement (y compris les actionnaires, les salariés, les clients et le grand public) les informations essentielles nécessaires pour leur permettre d'évaluer l'efficacité de l'organe de direction dans sa gestion de l'établissement.

Conformément à l'article 72 de la directive 2006/48/CE et à l'article 2 de la directive 2006/49/CE, les établissements mères de l'UE et les établissements contrôlés par une compagnie financière holding mère dans l'UE doivent communiquer des informations complètes et significatives pour décrire leur gouvernance interne à un niveau consolidé. Une bonne pratique consiste, pour chaque établissement, à communiquer de manière proportionnée des informations relatives à sa gouvernance interne sur une base individuelle.

2. L'établissement doit communiquer publiquement au moins les éléments suivants:

   a. ses structures et ses politiques de gouvernance, y compris ses objectifs, sa structure organisationnelle, ses mécanismes de gouvernance interne, la structure et l'organisation de l'organe de direction, y compris les règles de présence, ainsi que la structure des incitations et des rémunérations de l'établissement;

   b. la nature, la portée, la finalité et l'importance économique des transactions avec les filiales et d'autres parties liées, si celles-ci ont une incidence significative sur l'établissement;

   c. les modalités de la définition de la stratégie économique et en matière de risques (y compris la participation de l'organe de direction) et les facteurs de risque prévisibles;

   d. les comités mis en place, ainsi que leurs mandats et leur composition;

   e. le cadre de contrôle interne et l'organisation des fonctions de contrôle, les principales tâches qu'elles accomplissent, la manière dont leur performance est contrôlée par l'organe de direction et tout changement significatif prévu dans l'organisation de ces fonctions; et

   f. des informations significatives sur ses résultats financiers et opérationnels.

3. Les informations relatives à la situation actuelle de l'établissement doivent respecter les exigences légales en matière de communication d'informations. Ces dernières doivent être claires, précises, pertinentes, accessibles et fournies en temps utile.
4. Dans les cas où le fait d'assurer un haut degré de précision aurait pour effet de retarder la communication d'une information urgente, l'établissement doit juger de l'équilibre approprié entre la ponctualité et la précision, en tenant compte de l'obligation de donner une image sincère et fidèle de sa situation et de la nécessité de fournir une explication satisfaisante pour justifier tout retard. Cette explication ne peut pas servir de prétexte pour se conformer de manière tardive aux exigences périodiques de notification.

Titre III – Dispositions finales et mise en œuvre

34. Abrogation

Suite à l'adoption et à la publication des présentes orientations sur la gouvernance interne, les orientations suivantes sont abrogées: la section 2.1 des orientations du CECB sur l'application de la procédure de contrôle (en date du 25 janvier 2006), intitulée «Orientations sur la gouvernance interne», les «Principes de haut niveau relatifs aux politiques de rémunération» (en date du 20 avril 2009) et les «Principes de haut niveau relatifs à la gestion des risques» (en date du 16 février 2010).

35. Date d'application

Les autorités compétentes doivent mettre en œuvre les orientations sur la gouvernance interne en les intégrant dans leurs procédures de surveillance d'ici le 31 mars 2012. À compter de cette date, les autorités compétentes doivent veiller à ce que les établissements s'y conforment de manière effective.