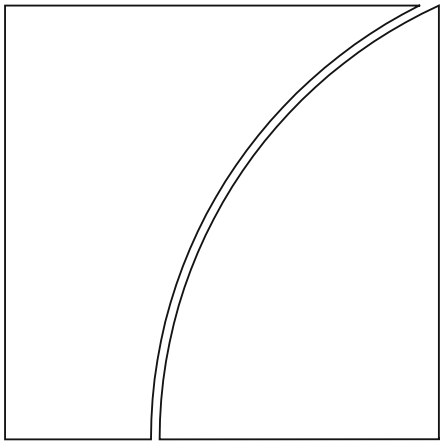
Comité de Bâle
sur le contrôle bancaire



Orientations

Principes de gouvernance d'entreprise à l'intention des banques

Juillet 2015

BANQUE DES RÈGLEMENTS INTERNATIONAUX

Le présent document est traduit de l'anglais. En cas de doute ou d'ambiguïté, se reporter à l'original (*Corporate governance principles for banks*).

Publication également disponible sur le site de la BRI (www.bis.org).

ISBN 978-92-9197-187-9 (en ligne)

Sommaire

Glossaire

administrateur dirigeant	Membre du conseil (par exemple, administrateur) qui exerce des fonctions de direction au sein de la banque[1] (il est à noter que certaines juridictions excluent cette possibilité). Au contraire, un **administrateur non dirigeant** est un membre du conseil qui n'exerce pas de fonctions de direction au sein de la banque.
administrateur indépendant	Aux fins du présent document, administrateur non dirigeant dont la capacité à exercer un jugement objectif n'est pas entravée par une quelconque influence, d'origine interne ou externe, de nature politique ou patrimoniale[1].
appétence pour le risque	Degré global et types de risques, préalablement fixés et inférieurs à la tolérance au risque, qu'une banque est disposée à assumer pour réaliser ses objectifs stratégiques et son plan d'activité[2].
banque, établissement bancaire	Toute banque, holding bancaire ou autre entreprise considérée par les autorités de contrôle bancaire comme étant la société mère d'un groupe bancaire en vertu de la législation nationale applicable selon le jugement de l'autorité de contrôle nationale.
conseil d'administration, conseil	Instance qui supervise la direction. La structure du conseil d'administration varie selon les pays[3]. Dans le présent document, les termes « conseil d'administration » et « conseil » recouvrent les différentes formes de conseils d'administration prévues par les législations nationales et doivent être interprétés conformément à la loi en vigueur dans la juridiction en question.
culture de l'entreprise en matière de risque, culture du risque	Normes, attitudes et conduites d'une banque relatives à la sensibilisation au risque, à la prise de risque et à la gestion des risques ainsi qu'à l'ensemble des contrôles qui orientent les décisions en matière de risque. La culture de l'entreprise en matière de risque influe sur les décisions de la direction et des employés dans l'accomplissement de leurs tâches quotidiennes et sur leur prise de risque[4].
déclaration d'appétence pour le risque	Énoncé écrit qui stipule l'appétence pour le risque. Il prévoit, d'une part, des critères quantitatifs exprimés en fonction des revenus, du niveau de fonds propres, des indicateurs de risque, de la liquidité et de tout autre grandeur pertinente et, d'autre part, des déclarations qualitatives concernant les risques de réputation et de conduite, ainsi que le blanchiment de capitaux et les pratiques contraires à l'éthique[5].
devoir de diligence	Obligation, pour tout administrateur, de prendre des décisions et d'agir de façon éclairée et prudente en ce qui concerne la société. Elle est souvent interprétée en ce sens qu'un administrateur est tenu de gérer les activités de la société comme le ferait une « personne prudente » pour ses propres affaires[6].

1 Voir Conseil de stabilité financière (CSF), *Thematic review on risk governance*, février 2013.

2 Voir CSF, *Principles for an effective risk appetite framework*, novembre 2013.

3 Voir paragraphe 15.

4 Voir CSF, *Guidance on supervisory interaction with financial institutions on risk culture*, avril 2014.

5 Voir CSF (novembre 2013), *op. cit.*

6 Voir le glossaire figurant dans Organisation de coopération et de développement économiques (OCDE), *Tables rondes régionales sur le gouvernement d'entreprise : Principaux enseignements*, 2003.

devoir de loyauté	Obligation, pour tout administrateur, d'agir en toute bonne foi dans l'intérêt de la société. En vertu de cette obligation, l'administrateur ne doit pas agir, dans son propre intérêt ou dans l'intérêt d'une personne ou d'un groupe, au détriment de la société et de l'ensemble de ses actionnaires[6].
dispositif d'appétence pour le risque	Ensemble des politiques, procédures, contrôles et systèmes qui permettent de définir, communiquer et surveiller l'appétence pour le risque. Il prévoit une déclaration d'appétence pour le risque, précise les plafonds de risque et décrit schématiquement les rôles et responsabilités des agents chargés de surveiller sa mise en œuvre. Il doit tenir compte des risques significatifs qui se présentent pour la banque dans son ensemble mais aussi pour sa réputation vis-à-vis de ses assurés, déposants, investisseurs et clients. Il est en adéquation avec la stratégie de la banque[7].
dispositif de gouvernance du risque	Composante du cadre global de gouvernance de l'entreprise dans laquelle s'inscrit l'instauration de la stratégie et de la politique de risque de la banque ; en outre, elle encadre les décisions du conseil et de la direction à ce sujet, explicite et surveille le respect de l'appétence pour le risque et des plafonds de risque par rapport à la stratégie de la banque, et enfin détecte, mesure, gère et maîtrise les risques[8].
fonctions de contrôle	Fonctions indépendantes de la direction chargées de mener des évaluations, d'informer et de donner des garanties de façon objective. Il s'agit notamment des fonctions gestion des risques, conformité et audit interne.
gestion des risques	Procédures mises en place afin que tout risque significatif et toute concentration de risque associée soient détectés, mesurés, limités, maîtrisés et atténués, et qu'il en soit rendu compte, de façon précoce et exhaustive.
gouvernance d'entreprise	Ensemble de relations entre la direction d'une entreprise, son conseil d'administration, ses actionnaires et d'autres parties prenantes, qui établissent le cadre dans lequel sont fixés les objectifs de la société ainsi que les moyens de les atteindre et d'en contrôler la réalisation[6]. La gouvernance d'entreprise contribue à définir l'attribution des pouvoirs et des responsabilités ainsi que les mécanismes de prise de décision.
plafonds de risque	Limites ou indicateurs quantitatifs et spécifiques, déterminés, par exemple, en fonction d'hypothèses prospectives qui répartissent le risque entre secteurs d'activité, entités juridiques (le cas échéant), catégories de risque spécifiques, concentrations et autres paramètres pertinents[2].
profil de risque	Évaluation ponctuelle des expositions au risque brutes d'une banque (c'est-à-dire avant l'application de mesures d'atténuation) ou, le cas échéant, des expositions au risque nettes (après atténuation), agrégées au sein des catégories de risque pertinentes et entre elles, sur la base d'hypothèses actuelles ou prospectives[2].
système de contrôles internes	Ensemble des règles et des contrôles qui régissent la structure organisationnelle et opérationnelle de la banque, y compris les procédures de notification et les fonctions gestion des risques, conformité et audit interne.
tolérance au risque	Niveau maximal de risque qu'une banque est en mesure d'assumer, étant donné ses fonds propres, sa gestion des risques, ses capacités de contrôle et ses contraintes réglementaires.

7 Voir CSF (novembre 2013), *op. cit*.

8 Voir CSF (février 2013), *op. cit*.

Principes de gouvernance d'entreprise à l'intention des banques

Introduction

1. Une gouvernance efficace est essentielle au bon fonctionnement du secteur bancaire et de l'économie dans son ensemble. Les banques jouent un rôle crucial dans l'économie en acheminant les fonds des épargnants et des déposants vers les activités qui contribuent au développement des entreprises et à la croissance économique. La sécurité et la solidité des banques étant des facteurs déterminants de la stabilité financière, la façon dont les banques mènent leurs activités est fondamentale pour la bonne santé de l'économie. En effet, lorsque la gouvernance de banques jouant un rôle important dans le système financier présente des points de fragilité, des difficultés peuvent se propager au secteur bancaire et à l'ensemble de l'économie.

2. La gouvernance d'entreprise doit avant tout viser à préserver de façon pérenne les intérêts des parties prenantes dans le respect de l'intérêt général. Parmi les parties prenantes, en particulier dans le cas des banques de détail, l'intérêt des déposants l'emporte sur celui des actionnaires.

3. La gouvernance d'entreprise détermine l'attribution des pouvoirs et des responsabilités du conseil d'administration et de la direction dans leur conduite des activités et opérations de la banque, notamment la façon dont ces organes :

- définissent la stratégie et les objectifs de la banque ;
- sélectionnent et supervisent le personnel ;
- mènent les activités de la banque au quotidien ;
- protègent les intérêts des déposants, s'acquittent de leurs obligations envers les actionnaires et prennent en compte les intérêts des autres parties prenantes ;
- adaptent la culture d'entreprise, les activités de la banque et son comportement afin que la banque soit dûment gérée de façon sûre, saine et intègre, dans le respect des lois et règlements applicables ;
- établissent les fonctions de contrôle.

4. Les présentes orientations proposées par le Comité de Bâle sur le contrôle bancaire (ci-après « le Comité de Bâle » ou « le Comité ») s'inspirent des principes de gouvernance d'entreprise publiés par l'Organisation de coopération et de développement économiques (OCDE). Les principes de l'OCDE, largement reconnus et établis de longue date, visent à aider les pouvoirs publics à évaluer et améliorer les règles régissant la gouvernance d'entreprise, et à fournir des recommandations aux autorités et aux acteurs des marchés financiers.

5. La bonne gouvernance d'entreprise intéresse au plus haut point les autorités de contrôle, car elle est indispensable à la sécurité et à la solidité d'une banque, et son dysfonctionnement pourrait altérer le profil de risque de la banque. En outre, la bonne gouvernance des banques contribue au maintien d'un processus de contrôle efficient et peu onéreux, puisqu'elle allège les besoins d'intervention des autorités prudentielles.

6. Une saine gouvernance permet aux autorités de contrôle de se fier davantage aux processus internes de la banque. D'après l'expérience des autorités, il est important que chaque banque dispose d'un système approprié de pouvoirs et de contre-pouvoirs, de responsabilités et d'obligations de rendre compte, au niveau non seulement du conseil d'administration mais aussi de la direction et des fonctions gestion des risques, conformité et audit interne.

7. Les principes publiés par le Comité de Bâle en octobre 2010 (*Principles for enhancing corporate governance*) s'inscrivaient dans les efforts que le Comité déploie depuis longtemps pour encourager les établissements bancaires à adopter de saines pratiques de gouvernance. Dans ce document, le Comité cherchait à intégrer les principaux enseignements de la crise financière mondiale qui s'est déclarée en 2007 et à renforcer la gouvernance des banques et la surveillance de ce domaine sensible par les autorités de contrôle.

8. Depuis 2010, le Comité et ses juridictions membres ont assisté au renforcement, par les banques, de leurs pratiques générales de gouvernance et à l'approfondissement, par les autorités de contrôle, de leurs processus de surveillance.

- En règle générale, les banques font preuve d'une meilleure compréhension des principaux aspects de la gouvernance d'entreprise : surveillance efficace du conseil d'administration, gestion rigoureuse des risques, stricts contrôles internes et mise en conformité, notamment. En outre, de nombreuses banques ont fait des progrès en ce qui concerne l'évaluation des aptitudes et des qualifications collectives du conseil d'administration, la mise en place au sein du conseil d'administration d'un comité de gestion des risques indépendant, la création et le renforcement du rôle de directeur de la gestion des risques et l'intégration de l'issue des consultations entre les comités du conseil chargé de l'audit et du suivi des risques.
- Les autorités nationales, quant à elles, ont pris des mesures pour améliorer la surveillance prudentielle et réglementaire de la gouvernance d'entreprise et du risque dans les banques. Elles ont notamment étoffé ou durci la règlementation ou les orientations existantes en la matière, renforcé leurs attentes à l'égard de la fonction gestion des risques, mené un dialogue plus nourri avec le conseil d'administration et la direction, et vérifié l'exactitude et l'utilité des informations fournies au conseil d'administration.

9. Afin de mesurer les progrès réalisés depuis la crise financière mondiale par les autorités nationales et le secteur bancaire en matière de gouvernance du risque, le Conseil de stabilité financière (CSF) a publié, en février 2013, un examen thématique sur le sujet, *Thematic review on risk governance*, dans le cadre de ses évaluations collégiales. Cet examen a montré que les établissements financiers et les autorités nationales avaient pris des mesures pour améliorer la gouvernance du risque. Tant les banques que les autorités nationales doivent néanmoins poursuivre leurs efforts afin de définir des dispositifs de gouvernance du risque efficaces et d'établir le cahier des charges de l'évaluation de ces dispositifs par les tiers. Les banques doivent également accroître les pouvoirs et l'indépendance des directeurs de la gestion des risques. Quant aux autorités nationales, elles doivent renforcer leurs capacités à évaluer l'efficacité de la gouvernance du risque et de la culture de l'entreprise en matière de risque (ci-après la « culture du risque »), et engager plus fréquemment des consultations avec le conseil d'administration et ses comités d'audit et de gestion des risques.

10. En raison des évolutions en cours dans la gouvernance d'entreprise et afin de tenir compte des recommandations de l'évaluation collégiale du CSF et d'autres travaux récents en la matière, le Comité a décidé de réexaminer ses orientations publiées en 2010[9].

11. L'un des principaux objectifs de la présente révision est de renforcer explicitement les responsabilités collectives du conseil d'administration en matière de surveillance et de gouvernance du

[9] Le CSF a recommandé que les juridictions membres renforcent leurs orientations réglementaires et prudentielles sur les saines pratiques de gouvernance du risque à l'intention des établissements financiers, en particulier des établissements financiers d'importance systémique (EFIS). En outre, le CSF a récemment publié des orientations supplémentaires, portant sur les dispositifs d'appétence pour le risque et sur les évaluations prudentielles de la culture du risque. Des travaux menés depuis 2010, notamment par l'Instance conjointe, ont eux aussi mis l'accent sur les enjeux de la supervision des groupes et des conglomérats. Ces travaux ont, à leur tour, soulevé d'importantes questions sur la gouvernance des groupes, notamment sur les attentes en matière de gouvernance de la société mère et de ses filiales, et sur les méthodes à adopter par les autorités de contrôle à l'égard de ces établissements.

risque. Un autre objectif est de mettre l'accent sur des composantes clés de la gouvernance du risque comme la culture du risque, l'appétence pour le risque et leurs liens avec la tolérance au risque d'une banque. Les nouvelles orientations définissent les attributions précises du conseil d'administration, du comité du conseil chargé des risques, de la direction et des fonctions de contrôle, dont celles du directeur de la gestion des risques et de l'audit interne. Enfin, elles visent également à renforcer l'équilibre global des pouvoirs dans les banques.

12. Il est à noter que le CSF a souligné le rôle central joué par le conseil d'administration et son comité des risques dans le renforcement de la gouvernance du risque au sein des banques. Ce renforcement suppose une plus grande implication dans l'évaluation et la promotion d'une solide culture du risque au sein de l'établissement ; la définition du niveau d'appétence pour le risque et son expression dans la déclaration d'appétence pour le risque ; et la surveillance de la mise en œuvre par la direction du dispositif d'appétence pour le risque et du dispositif général de gouvernance du risque.

13. L'importance croissante accordée au risque et au dispositif de gouvernance du risque porte notamment sur la définition des responsabilités des différentes composantes de l'organisation dans le traitement et la gestion des risques. Souvent dénommées les « trois lignes de défense », elles ont chacune un rôle important à jouer. La ligne opérationnelle, première ligne de défense, est responsable de la prise en compte et de la maîtrise des risques auxquels ses activités donnent lieu. Deuxième ligne de défense, indépendante de la première, la fonction gestion des risques est chargée de détecter, mesurer et suivre les risques à l'échelle de l'entreprise, et d'en rendre compte. La fonction conformité relève également de la deuxième ligne de défense. Quant à la troisième ligne de défense, elle est assurée par la fonction audit interne, qui conduit à ce titre des audits et des examens axés sur le risque, mais aussi de portée plus générale, afin de donner au conseil d'administration l'assurance que le cadre général de gouvernance, y compris le dispositif de gouvernance du risque, est efficace et que des politiques et processus sont en place à cet effet et sont appliqués de façon cohérente.

14. L'une des attributions du conseil d'administration et de la direction est de définir les comportements à risque dans le contexte des activités de la banque[10]. Les comportements répréhensibles peuvent résulter de :

- la vente abusive de produits financiers aux particuliers et aux entreprises ;
- la violation de lois nationales et internationales (législation fiscale, règles anti-blanchiment et anti-terrorisme, sanctions économiques, notamment) ;
- la manipulation des marchés financiers (par exemple, la manipulation du Libor et des taux de change).

Le conseil doit donner l'exemple « d'en haut » et veiller à ce que la direction remplisse son rôle d'encouragement et de maintien d'une saine culture d'entreprise et d'une solide culture du risque. La direction doit rédiger un code déontologique ou un code de conduite visant à favoriser une culture de l'intégrité et de la responsabilité afin de protéger les intérêts des clients et des actionnaires.

Différences entre juridictions

15. Les présentes orientations visent à guider l'action des membres du conseil d'administration et de la direction, des responsables des fonctions de contrôle et des superviseurs d'un large éventail de banques

[10] Voir Groupe des trente, *Banking Conduct and Culture: a Call for Sustained and Comprehensive Reform*, juillet 2015, et Comité européen du risque systémique (CERS), *Report on misconduct risk in the banking sector*, juin 2015.

dans des juridictions, membres ou non du Comité de Bâle, dotées de systèmes juridiques et réglementaires très différents. Le Comité est conscient que ces systèmes recouvrent une grande diversité de configurations, qui pourrait limiter l'application de certains principes ou dispositions figurant dans le présent document. Chaque juridiction doit appliquer les dispositions que les autorités nationales estiment pertinentes. Il conviendra alors dans certains cas de modifier la loi et, dans d'autres, d'adapter légèrement un principe.

Applicabilité, proportionnalité et différences des approches en matière de gouvernance

16. La mise en œuvre de ces principes doit être adaptée à la taille, à la complexité, à la structure, au poids économique, au profil de risque et au modèle opérationnel de la banque et, le cas échéant, du groupe auquel elle appartient. Il conviendra donc de procéder à des ajustements raisonnables, si nécessaire, pour les banques dont le profil de risque est faible, et d'être attentif aux risques accrus que les banques cotées et les établissements plus complexes peuvent présenter[11]. Un établissement financier d'importance systémique (EFIS) doit ainsi disposer d'une structure et de pratiques de gouvernance d'entreprise adaptées à son envergure et aux répercussions que sa défaillance pourrait avoir sur la stabilité financière nationale et mondiale.

17. Les présents principes sont pertinents pour toute juridiction, qu'elle ait choisi ou non d'adopter le cadre réglementaire du Comité. Il incombe au conseil d'administration et à la direction de la banque d'œuvrer à la bonne gouvernance de l'établissement.

18. Le présent document se réfère à une structure de gouvernance composée d'un conseil d'administration et d'une direction. La « direction » peut désigner des entités dénommées « comité de direction », « conseil exécutif » ou « comité de gestion ». Ainsi, dans certains pays, les banques ont une structure à deux niveaux, dans laquelle la fonction de surveillance du conseil d'administration est attribuée à un organe distinct, appelé « conseil de surveillance » ou « conseil de surveillance et d'audit », qui n'a aucune fonction exécutive. Dans d'autres pays, le conseil d'administration est l'organe unique et il joue un rôle plus étendu. D'autres pays encore ont opté pour une approche mixte ou s'orientent vers ce type d'approche. Dans ces pays, il est impossible ou déconseillé d'exercer des fonctions exécutives et de siéger au conseil d'administration, ou bien le nombre de responsables exécutifs au conseil d'administration est limité, ou encore la présidence du conseil ou des comités du conseil ne peut être assurée que par un administrateur non dirigeant ou indépendant. Certains pays interdisent en outre au directeur général de présider le conseil d'administration, voire d'en être membre.

19. Du fait de ces disparités, les présentes orientations ne préconisent aucune forme précise de conseil d'administration ou de structure de gouvernance. Les termes « conseil d'administration » et « direction » sont ici principalement utilisés dans l'optique d'une structure à instance unique, mais ils doivent être, dans la totalité du document, interprétés conformément à la loi applicable dans chaque juridiction. Conscient que différentes structures de gouvernance d'entreprise existent et qu'elles évoluent avec le temps, le Comité encourage les législateurs, les autorités de contrôle, les banques et les autres parties concernées à passer régulièrement en revue leurs pratiques afin de renforcer les mécanismes régulateurs et la solidité de la gouvernance d'entreprise, quelle que soit la structure en place. Il va de soi

[11] Le Comité est conscient que certains pays ont adopté, pour les grands établissements et les sociétés cotées, des normes de gouvernance, de comptabilité et d'audit plus complètes et plus prescriptives que les présents principes.

que la mise en œuvre des normes de gouvernance d'entreprise doit respecter les lois, règlements et codes applicables dans la juridiction en question (et donc, le cas échéant, tenir compte de l'existence d'un conseil de surveillance).

20. Les droits des actionnaires constituent l'un des aspects les plus importants de la gouvernance d'entreprise des sociétés cotées. Les présentes orientations ne portent pas principalement sur ces droits, qui sont l'objet des principes de gouvernance publiés par l'OCDE[12]. Néanmoins, le Comité reconnaît l'importance de ces droits, tout comme celle que revêt l'engagement responsable des actionnaires. Ainsi, il considère essentiel que les actionnaires exercent leurs droits, en particulier celui dont jouissent certains actionnaires de désigner un représentant au conseil d'administration. Il est important que ce représentant ait les aptitudes et les qualifications nécessaires mais aussi qu'il comprenne bien quelle est sa principale mission : veiller aux intérêts de la banque dans son ensemble et pas seulement à ceux des actionnaires.

21. Pour être mise en œuvre efficacement, une saine gouvernance d'entreprise doit s'appuyer sur des bases législatives, réglementaires et institutionnelles adaptées. Toute une série de facteurs, dont la configuration du droit des affaires, des règles boursières et des normes comptables, peut avoir une incidence sur l'intégrité des marchés et la stabilité du système financier. Or, bien souvent, ces facteurs ne sont pas du ressort du contrôle bancaire. Néanmoins, les autorités de contrôle sont invitées à se tenir informées des obstacles juridiques et institutionnels en la matière et, quand elles y sont légalement habilitées, à prendre des mesures favorisant l'instauration de fondements robustes pour une saine gouvernance d'entreprise. Lorsque ce n'est pas le cas, les autorités de contrôle souhaiteront peut-être soutenir des réformes législatives ou d'autres mesures qui leur permettraient d'encourager ou d'imposer plus directement une saine gouvernance d'entreprise.

22. Les principes de saine gouvernance d'entreprise s'appliquent également aux banques publiques et aux banques aidées par l'État, même lorsque cette aide est temporaire[13].

[12] OCDE, *Principes de gouvernement d'entreprise de l'OCDE*, 2004 : www.oecd.org/fr/daf/ae/principesdegouvernementdentreprise/31652074.PDF. En 2014, l'OCDE a entrepris la révision de ces principes afin de s'assurer de leur qualité, pertinence et utilité, au vu de l'évolution récente du secteur des entreprises et des marchés des capitaux : http://www.oecd.org/daf/ca/Corporate-Governance-Principles-FRA.pdf.

[13] Voir OCDE, *Lignes directrices de l'OCDE sur la gouvernance des entreprises publiques*, www.oecd.org/fr/daf/ae/ocde-lignes-directrices-gouvernement-entreprises-publiques.htm.

Principe 1 – Responsabilités générales du conseil d'administration

Le conseil d'administration a la responsabilité globale de la banque ; il est en particulier chargé d'approuver et de surveiller la mise en œuvre, par la direction, des objectifs stratégiques, du cadre de gouvernance et de la culture d'entreprise.

Responsabilités du conseil d'administration

23. Le conseil d'administration est responsable en dernier ressort de la stratégie opérationnelle et de la santé financière de la banque, des décisions clés concernant les ressources humaines, de l'organisation interne, de la structure et des pratiques de gouvernance, de la gestion des risques et du respect de la conformité. Le conseil peut, si nécessaire, déléguer certaines de ses fonctions – mais non ses responsabilités – à des comités désignés en son sein.

24. Le conseil doit établir la structure organisationnelle de la banque à sa satisfaction. L'objectif est que le conseil et la direction puissent assumer leurs responsabilités et que la prise de décision soit efficace, et la gouvernance, de bonne qualité. Pour ce faire, le conseil doit notamment définir clairement ses principaux pouvoirs et responsabilités, ainsi que ceux de la direction, de la fonction gestion des risques et des autres fonctions de contrôle.

25. Les membres du conseil doivent exercer leur devoir de diligence et leur devoir de loyauté envers la banque dans le cadre des lois nationales et des normes prudentielles en vigueur.

26. Par conséquent, le conseil d'administration doit[14] :

- s'impliquer activement dans les activités de la banque, se tenir informé des faits nouveaux importants survenant dans l'environnement opérationnel de la banque et sur le plan économique, et agir en temps opportun pour protéger les intérêts à long terme de la banque ;
- surveiller[15] l'élaboration des objectifs opérationnels et de la stratégie de la banque, les approuver et en suivre la mise en œuvre ;
- jouer un rôle de chef de file dans l'instauration des valeurs et de la culture d'entreprise de la banque ;
- surveiller la mise en œuvre du cadre de gouvernance et vérifier régulièrement sa pertinence au regard de changements importants dans la taille de la banque, sa complexité, son implantation géographique, sa stratégie opérationnelle, les marchés et les exigences réglementaires ;
- établir, conjointement avec la direction et le directeur de la gestion des risques, l'appétence de la banque pour le risque, en tenant compte de l'environnement concurrentiel et réglementaire ainsi que des intérêts à long terme de la banque, de son exposition au risque et de sa capacité à gérer efficacement les risques ;
- surveiller le respect de la déclaration d'appétence pour le risque, de la politique à l'égard du risque et des plafonds de risque ;
- approuver l'approche choisie et surveiller la mise en œuvre des principales politiques relatives au processus d'évaluation de l'adéquation des fonds propres, des plans de liquidité et de fonds

[14] Le Comité est conscient que, dans certaines juridictions, ces questions sont régies par des normes découlant du droit des sociétés et que les autorités de contrôle nationales tiennent dûment compte de ces normes pour l'application des présents principes.

[15] Dans le contexte des responsabilités du conseil, le terme « surveiller » a le sens de « surveiller et être satisfait de ».

propres, des politiques et obligations en matière de conformité, et du système de contrôles internes ;

- exiger la présence d'une solide fonction finances, responsable de la comptabilité et des données financières ;
- approuver les états financiers annuels et demander une évaluation indépendante régulière des éléments les plus importants ;
- approuver le choix et surveiller la performance du directeur général, des principaux membres de la direction et des responsables des fonctions de contrôle ;
- surveiller la politique de rémunération de la banque, et notamment la rémunération des directeurs pour vérifier sa conformité avec la culture du risque de la banque et son appétence pour le risque ;
- surveiller l'intégrité, l'indépendance et l'efficacité des politiques et des procédures de la banque en matière de lancement d'alerte.

27. Le conseil d'administration doit veiller à ce que les transactions avec des parties liées (dont les transactions intragroupes) fassent l'objet d'une évaluation des risques et de restrictions appropriées (en exigeant par exemple qu'elles respectent les conditions de concurrence normales), et que les ressources de l'entreprise ne soient pas détournées ou mal utilisées.

28. Dans l'exécution de ses responsabilités, le conseil d'administration doit tenir dûment compte des intérêts légitimes des déposants, des actionnaires et des autres parties prenantes. Il doit également veiller à ce que la banque entretienne de bonnes relations avec les autorités de contrôle.

Valeurs et culture de l'entreprise

29. Une culture d'entreprise valorisant un comportement responsable et éthique constitue un élément essentiel de la bonne gouvernance. Ces valeurs jouent un rôle particulièrement important dans la sensibilisation au risque, la prise de risque et la gestion des risques (c'est-à-dire la culture du risque).

30. Afin de promouvoir une saine culture d'entreprise, le conseil d'administration doit montrer l'exemple, c'est-à-dire :

- définir un système de valeurs supposant que toutes les activités de la banque sont menées dans le respect de la légalité et de l'éthique, adhérer à ces valeurs et surveiller leur observance par la direction et le personnel ;
- favoriser une sensibilisation au risque par une solide culture du risque, transmettant ses attentes, à savoir qu'il ne souscrit pas à une prise de risque excessive et que chacun doit faire en sorte que les activités de la banque respectent l'appétence pour le risque et les plafonds de risque fixés ;
- confirmer que des mesures appropriées ont été prises ou sont prises pour communiquer à l'intérieur de la banque le système de valeurs, les normes professionnelles et les codes de conduite qu'il a établis, ainsi que des politiques d'accompagnement adéquates ;
- attester que l'ensemble du personnel, y compris la direction, est au fait des mesures, disciplinaires notamment, qui s'appliquent en cas de comportements inacceptables et d'infractions.

31. Un code de conduite ou un code déontologique doit définir les comportements acceptables et inacceptables au sein de la banque.

- Il doit ainsi interdire explicitement toute activité illégale, comme les fausses déclarations financières, les comportements financiers répréhensibles, la délinquance économique, et notamment la fraude, la violation de sanctions, le blanchiment de capitaux, les pratiques

anticoncurrentielles et la corruption active et passive, ou encore les violations des droits du consommateur.

- Il doit en outre stipuler que les employés sont tenus d'adopter un comportement éthique et d'accomplir leurs fonctions professionnelles avec compétence et diligence dans le respect de la législation, de la réglementation et des politiques de l'entreprise.

32. Le système de valeurs de la banque doit accorder une importance essentielle à l'instauration d'un dialogue franc et en temps opportun en cas de problèmes, et au signalement de ces cas aux niveaux hiérarchiques supérieurs de l'organisation.

- Les employés doivent être encouragés à exprimer leurs préoccupations légitimes concernant des pratiques illégales, contraires à la déontologie ou douteuses, et avoir la possibilité d'exprimer ces suspicions sous le sceau de la confidentialité et sans crainte de représailles. Cela sera plus facile si la banque applique une politique clairement explicitée en la matière ainsi que des procédures et processus adéquats, conformes à la loi nationale, qui permettent aux employés de faire part de leurs préoccupations et observations légitimes et sérieuses concernant toute violation des règles, en toute confidentialité (politique relative au lancement d'alerte, par exemple), tant au sein de la banque qu'à l'autorité de contrôle.
- Le conseil d'administration doit surveiller la politique de lancement d'alerte et s'assurer que la direction donne suite aux questions légitimement soulevées. Il est tenu de s'assurer que les employés qui signalent des problèmes sont protégés de toutes représailles et de tout traitement préjudiciable.
- Le conseil d'administration doit surveiller et approuver la procédure d'investigation et de traitement des préoccupations légitimes et sérieuses par une instance objective, indépendante, intérieure ou extérieure, par la direction ou par le conseil d'administration lui-même.

Appétence pour le risque, gestion et contrôle des risques

33. Au sein du cadre général de gouvernance de la banque, le conseil d'administration est tenu de surveiller la mise en œuvre d'un dispositif de gouvernance du risque rigoureux. Pour être efficace, ce dispositif suppose l'existence d'une solide culture du risque, d'une appétence pour le risque pertinente, explicitée dans la déclaration d'appétence pour le risque, et de fonctions clairement définies pour ce qui est de la gestion des risques en particulier et des fonctions de contrôle en général.

34. Il est essentiel d'établir et de faire connaître l'appétence pour le risque afin de consolider la culture du risque. Le dispositif de gouvernance du risque doit définir les mesures à prendre en cas de dépassement des plafonds de risque : mesures disciplinaires en cas de prise de risque excessive, alerte des niveaux hiérarchiques supérieurs et notification du conseil d'administration, notamment.

35. Le conseil d'administration doit jouer un rôle actif dans la définition de l'appétence pour le risque et veiller à sa concordance avec la stratégie, le plan financier, la gestion des fonds propres et les pratiques de la banque en matière de rémunération. L'appétence pour le risque doit être clairement expliquée dans une déclaration d'appétence pour le risque aisément compréhensible par toutes les parties concernées : conseil d'administration, direction, employés de la banque et autorité de contrôle.

36. La déclaration d'appétence pour le risque doit :

- comporter des éléments tant quantitatifs que qualitatifs ;
- déterminer le degré global et individuel et les types de risque, préalablement fixés et inférieurs à la tolérance au risque, que la banque est prête à assumer pour réaliser son plan d'activité ;
- définir les limites et les conditions d'exploitation dans lesquelles la banque est supposée poursuivre sa stratégie opérationnelle ;

- faire connaître à tous les services et échelons de la banque l'appétence pour le risque établie par le conseil d'administration, en la rattachant à la prise de décision au quotidien et en prévoyant les moyens de faire part de questions et de préoccupations concernant les risques et la stratégie de la banque.

37. L'élaboration d'une déclaration d'appétence pour le risque doit s'appuyer sur la synergie d'une double dynamique, l'une émanant du conseil d'administration et l'autre de la direction. L'appétence pour le risque peut certes être définie à l'initiative de la direction, mais l'efficacité de sa mise en œuvre dépend, elle, de la qualité des interactions entre différents groupes : le conseil d'administration, la direction, l'unité de gestion des risques et les services opérationnels, dont le directeur financier.

38. Le dispositif de gouvernance du risque doit clairement situer la responsabilité de la gestion des risques au sein de l'organisation, ce qui est généralement désigné par les « trois lignes de défense » :

- la ligne opérationnelle ;
- les fonctions gestion des risques et conformité, indépendantes de la première ligne de défense ;
- la fonction audit interne, indépendante des deux premières lignes de défense[16].

39. La structure précise de ces trois lignes de défense peut varier selon la nature, la taille, la complexité et le profil de risque de la banque. Dans tous les cas, les responsabilités au sein de chacune de ces lignes de défense doivent être bien définies et bien communiquées.

40. Les départements opérationnels de la banque constituent la première ligne de défense. Ils prennent des risques, ils sont responsables de la gestion courante de ces risques et ils doivent en rendre compte. À ce titre, ils sont tenus de détecter, d'évaluer et de signaler ces expositions, en tenant compte de l'appétence pour le risque de la banque et des politiques, procédures et contrôles en la matière. La ligne opérationnelle doit s'acquitter de ses missions conformément à la culture du risque en vigueur. Le conseil d'administration doit promouvoir une solide culture de respect des seuils fixés et de gestion des expositions au risque.

41. Une fonction gestion des risques indépendante est l'un des éléments constitutifs de la deuxième ligne de défense. Responsable du suivi des risques et chargée d'en rendre compte, cette fonction complète la première ligne de défense. Il lui incombe notamment de surveiller les activités comportant une prise de risque et d'évaluer les risques et les problèmes éventuels, indépendamment de la ligne opérationnelle. Elle doit mettre l'accent sur l'importance du rôle joué par la direction et les responsables des départements opérationnels dans la détection et l'évaluation des risques, et non s'en tenir uniquement à la surveillance assurée par l'équipe de gestion des risques. La fonction finances, entre autres, joue un rôle de premier plan en veillant à ce que les performances opérationnelles et les résultats financiers soient correctement enregistrés et communiqués au conseil d'administration, à la direction et aux unités opérationnelles, pour lesquels ces informations seront des éléments clés de leurs décisions en matière de risque et d'activités opérationnelles.

42. La deuxième ligne de défense repose également sur une fonction conformité indépendante et performante. Cette fonction doit notamment vérifier régulièrement que la banque respecte les lois, règles de gouvernance, règlementations, codes et politiques auxquels elle est soumise. Le conseil d'administration doit approuver les politiques de conformité, qui sont communiquées à l'ensemble des employés. La fonction conformité doit évaluer dans quelle mesure les politiques sont observées et rendre compte à la direction, et le cas échéant au conseil d'administration, de la façon dont la banque gère le risque de non-conformité. En outre, elle doit être dotée de l'autorité, de la stature, de l'indépendance et

[16] Voir Comité de Bâle sur le contrôle bancaire, *Principles for sound operational risk management*, juin 2011, www.bis.org/publ/bcbs195.pdf, et *The internal audit function in banks*, juin 2012, www.bis.org/publ/bcbs223.pdf.

des ressources nécessaires à ses missions, et pouvoir entrer librement en relation avec le conseil d'administration.

43. La troisième ligne de défense est constituée d'une fonction audit interne indépendante et efficace. Cette fonction fournit un examen indépendant et une assurance objective de la qualité et de l'efficacité du système de contrôles internes de la banque, des première et deuxième lignes de défense et du dispositif de gouvernance du risque (notamment ses liens avec la culture organisationnelle), ainsi que des processus relatifs aux plans stratégique et d'activité, à la rémunération et à la prise de décision. Les auditeurs internes doivent être compétents et correctement formés. En outre, ils ne doivent pas participer à l'élaboration, à la mise en œuvre ou à l'exécution de la fonction gestion des risques ni des fonctions incluses dans les deux premières lignes de défense (Principe 9).

44. Le conseil d'administration doit faire en sorte que les fonctions gestion des risques, conformité et audit interne disposent du statut et des ressources humaines et économiques nécessaires, et qu'elles s'acquittent de leurs missions de façon efficace, en toute indépendance et objectivité. Dans le cadre de sa mission de surveillance du cadre de gouvernance du risque, le conseil d'administration doit procéder à un examen régulier des principaux contrôles et politiques, conjointement avec la direction et les responsables des fonctions gestion des risques, conformité et audit interne, afin de détecter et de traiter les risques et les problèmes importants et de déterminer les points à améliorer.

Surveillance de la direction

45. Il incombe au conseil d'administration de choisir, à l'issue d'un processus de sélection, le directeur général et éventuellement d'autres membres importants du personnel, comme les membres de la direction.

46. La surveillance de la direction doit incomber au conseil d'administration. Celui-ci doit tenir la direction pour responsable de ses actes et expliciter les conséquences (y compris la révocation) auxquelles elle s'expose si elle ne se conforme pas aux attentes du conseil en termes de performance. En particulier, la direction est tenue, en toutes circonstances, de respecter les valeurs, l'appétence pour le risque et la culture du risque de la banque. Pour ce faire, le conseil d'administration doit :

- vérifier que la direction agit conformément à la stratégie et aux politiques qu'il a approuvées, notamment l'appétence pour le risque ;
- se réunir régulièrement avec la direction ;
- remettre en cause et examiner d'un œil critique les explications et les informations fournies par la direction ;
- fixer, pour la direction, des objectifs de performance et des niveaux de rémunération adéquats et cohérents avec la stratégie à long terme et la solidité financière de la banque ;
- déterminer si les connaissances et les compétences collectives de la direction restent adaptées à la nature des activités de la banque et à son profil de risque ;
- participer activement à l'élaboration des plans de succession pour le directeur général et d'autres postes clés, en tant que de besoin, et veiller à la mise en place de plans de succession pour les membres de la direction.

Principe 2 – Composition et qualifications du conseil d'administration

Les membres du conseil d'administration doivent, individuellement et collectivement, posséder, à tout moment, les qualifications voulues pour remplir leurs missions. Ils doivent être conscients de leur rôle en matière de surveillance et de gouvernance et être capables de porter un jugement avisé et objectif sur les activités de la banque.

Composition du conseil d'administration

47. Le conseil d'administration doit être à même d'exercer ses fonctions et sa composition doit permettre une surveillance efficace. À cette fin, le conseil d'administration doit compter un nombre suffisant d'administrateurs indépendants.

48. Le conseil d'administration doit être composé de personnes qui présentent une combinaison équilibrée d'aptitudes, de diversité et d'expérience et qui, collectivement, possèdent les qualifications nécessaires, compte tenu de la taille, de la complexité et du profil de risque de la banque.

49. Il convient de tenir compte des critères suivants pour déterminer si le conseil d'administration dans son ensemble détient les qualifications voulues :

- afin de favoriser la pluralité des points de vue, les membres du conseil d'administration doivent disposer de connaissances variées et d'une vaste expérience dans des domaines d'intérêt pour la banque et avoir suivi des parcours différents. Parmi les domaines de compétence pertinents figurent, entre autres, les marchés de capitaux, l'analyse financière, les questions de stabilité financière, l'information financière, les technologies de l'information, la planification stratégique, la gestion des risques, les politiques de rémunération, la règlementation, la gouvernance d'entreprise et la gestion ;
- le conseil d'administration pris dans son ensemble doit avoir une compréhension raisonnablement bonne de l'économie et des marchés à l'échelle locale, régionale et, si nécessaire, mondiale, ainsi que de l'environnement légal et réglementaire. S'il y a lieu, une expérience internationale doit également être prise en compte ;
- par son attitude, chaque membre du conseil d'administration doit faciliter la communication, la collaboration et le débat critique dans le processus de décision.

Processus de sélection et qualifications des membres du conseil

50. Chaque conseil d'administration doit être doté d'un processus clair et rigoureux d'identification, d'évaluation et de sélection des candidats. Sauf disposition légale contraire, le conseil d'administration (et non la direction) désigne[17] les candidats et encourage l'élaboration d'un plan adéquat de succession de ses membres.

51. Il convient de s'assurer, durant le processus de sélection, que les candidats : i) possèdent les connaissances, les compétences, l'expérience et, en particulier dans le cas des administrateurs non dirigeants, l'indépendance nécessaires à leurs fonctions compte tenu des activités et du profil de risque de la banque ; ii) ont des antécédents caractérisés par l'intégrité et une bonne réputation ; iii) disposent

[17] Le Comité est conscient que, dans certaines juridictions, les actionnaires ou d'autres parties prenantes ont le droit de désigner des membres du conseil ou d'approuver leur désignation. Dans ce cas aussi, le conseil d'administration doit faire tout ce qui est en son pouvoir pour s'assurer que les membres sélectionnés sont qualifiés pour le poste.

du temps suffisant pour exercer pleinement leurs responsabilités et iv) ont les qualités requises pour favoriser une bonne interaction entre les membres du conseil.

52. Aucun conflit d'intérêts ne doit entraver la capacité des candidats à exercer leurs fonctions en toute indépendance et objectivité ni les soumettre à une influence illégitime :

- émanant d'autres personnes (membres de la direction ou actionnaires, par exemple) ;
- résultant de postes actuels ou occupés par le passé ;
- procédant de relations de nature personnelle, professionnelle ou économique avec des membres du conseil d'administration ou de la direction (ou avec d'autres entités du groupe).

53. Si un membre du conseil d'administration en vient à ne plus détenir les compétences nécessaires à l'exercice de ses fonctions ou à ne plus assumer correctement ses responsabilités, le conseil doit prendre les mesures qui s'imposent dans le respect de la loi (par exemple, en informer l'autorité de contrôle bancaire).

54. La banque doit disposer d'un comité des nominations, ou d'un organe semblable, qui comprenne un nombre suffisant d'administrateurs indépendants et qui sélectionne et désigne les candidats en tenant compte des critères énoncés plus haut. Le comité des nominations et les autres comités du conseil sont présentés plus en détail au paragraphe 77.

55. Pour permettre aux membres du conseil d'administration d'acquérir, de tenir à jour et d'approfondir les connaissances et les compétences requises et de bien s'acquitter de leurs responsabilités, le conseil doit veiller à ce que ses membres participent à une formation à leur arrivée et puissent accéder à une formation continue sur des questions d'intérêt pour la banque, ce qui peut mobiliser des ressources internes ou externes. Le conseil doit consacrer le temps et les ressources, financières notamment, nécessaires à la réalisation de cet objectif de formation et faire appel à des spécialistes externes si besoin. Des efforts plus importants doivent être déployés pour offrir une formation et une actualisation des connaissances aux membres ayant une expérience plus limitée dans le domaine financier et en matière de risque et de réglementation.

56. Lorsque les actionnaires ont le droit de nommer des membres du conseil d'administration, celui-ci doit s'assurer que ces personnes comprennent bien leurs obligations. Les membres du conseil d'administration ont des responsabilités vis-à-vis des intérêts de la banque dans son ensemble, indépendamment de l'instance qui les nomme. Dans le cas où des membres du conseil d'administration sont désignés par un actionnaire détenant une majorité de contrôle, le conseil d'administration souhaitera peut-être mettre en place des procédures spécifiques ou mener des examens périodiques pour s'assurer que les missions du conseil sont dûment remplies par l'ensemble des membres.

Principe 3 – Structure et pratiques du conseil d'administration

Le conseil d'administration doit définir, pour ses propres travaux, des structures et des pratiques de gouvernance appropriées, se doter des moyens nécessaires au respect de ces pratiques et les passer régulièrement en revue pour s'assurer de leur efficacité.

Organisation et évaluation du conseil d'administration

57. Le conseil d'administration doit décider de sa configuration, et notamment de sa direction, de sa taille ainsi que du recours éventuel à des comités, de façon à remplir efficacement son rôle de surveillance et ses autres missions. Il doit en particulier s'assurer qu'il dispose du temps et des moyens nécessaires pour accorder à tous les sujets l'importance qu'ils méritent et procéder à un examen circonstancié des problèmes.

58. Le conseil d'administration doit mettre régulièrement à jour les règles, les statuts et les autres documents qui régissent son organisation, ses droits, ses responsabilités et ses principales activités.

59. À l'appui de ses propres performances, le conseil d'administration doit mener une évaluation régulière du conseil dans son ensemble, de ses comités et de chacun de ses membres, seul ou avec l'aide d'experts extérieurs. Le conseil d'administration doit ainsi :

- passer régulièrement en revue sa structure, sa taille et sa composition ainsi que la structure et la coordination des comités ;
- vérifier périodiquement (au moins une fois par an) que chacun de ses membres reste qualifié pour le poste qu'il occupe, en tenant compte de sa performance au sein du conseil ;
- procéder, lors de ces contrôles ou indépendamment, à des examens périodiques de l'efficacité de ses pratiques et procédures de gouvernance, déterminer les points à améliorer et effectuer tout changement nécessaire ;
- s'appuyer sur les conclusions de ces évaluations pour poursuivre ses efforts d'amélioration, et communiquer à l'autorité de contrôle lesdites conclusions si elle en fait la demande.

60. Le conseil d'administration doit tenir un registre approprié de ses délibérations et décisions (sous forme de procès-verbaux des réunions ou de comptes rendus sommaires des questions abordées, des recommandations formulées, des décisions prises et des opinions divergentes exprimées). Il doit les transmettre à l'autorité de contrôle, si elle en fait la demande.

Rôle du président

61. Le président du conseil d'administration joue un rôle essentiel dans la bonne marche de celui-ci. Il pilote les activités du conseil d'administration et il est chargé d'en assurer le bon fonctionnement, notamment en entretenant une relation de confiance avec ses membres. Il doit posséder l'expérience, les compétences et les qualités personnelles nécessaires pour s'acquitter de ces missions. Il doit veiller à ce que les décisions prises par le conseil d'administration reposent sur des principes sains et soient suffisamment étayées. Il doit encourager le débat et veiller à ce que les avis divergents puissent être librement exprimés et examinés dans le processus de prise de décision. Il doit consacrer suffisamment de temps à l'exercice de ses responsabilités.

62. Afin de favoriser l'équilibre des pouvoirs, le président du conseil doit être un administrateur indépendant ou un administrateur non dirigeant. Dans les juridictions où le président du conseil peut exercer des fonctions de direction, la banque doit adopter des mesures afin que cette situation ne nuise pas à l'équilibre des pouvoirs, par exemple en désignant un membre du conseil en chef ou un

administrateur indépendant principal, et en accroissant le nombre d'administrateurs non dirigeants siégeant au conseil.

Comités du conseil

63. Pour accroître son efficacité et approfondir des domaines précis, le conseil d'administration peut créer des comités spécialisés en son sein. La création de ces comités et la définition de leur mandat doivent être décidées en séance plénière. Le nombre et la nature des comités dépendent de différents facteurs, comme la taille de la banque et de son conseil d'administration, la nature des activités et le profil de risque de la banque.

64. Chaque comité doit disposer d'une charte ou de tout autre document définissant son mandat, le champ de ses activités et ses règles de fonctionnement. Ce document doit notamment prévoir la façon dont le comité rend compte de ses activités au conseil réuni en séance plénière, les attentes à l'égard de ses membres et, le cas échéant, la durée maximale de leur mandat. Le conseil d'administration doit envisager l'adoption d'un système de rotation périodique des sièges et de la présidence de ces comités, afin d'éviter une concentration injustifiée des pouvoirs et de permettre l'expression de nouveaux points de vue.

65. Dans un souci de transparence, le conseil d'administration doit rendre publics le mandat et la composition de ses comités (y compris les membres considérés comme indépendants).

66. Les comités doivent tenir le registre de leurs délibérations et de leurs décisions (sous forme de procès-verbaux des réunions ou de comptes rendus des questions abordées, des recommandations formulées, décisions prises et opinions divergentes exprimées). Ces registres doivent rendre compte de la façon dont les comités s'acquittent de leur mission, et permettre aux autorités de contrôle, ou autre instance responsable, d'évaluer le fonctionnement des comités.

67. Les comités du conseil doivent être présidés par des administrateurs indépendants, non dirigeants.

Comité d'audit

68. Un comité d'audit doit[18] :

- être obligatoire dans toute banque d'importance systémique ; pour les autres banques, il est fortement recommandé, selon la taille, le profil de risque et la complexité de la banque ;
- être distinct des autres comités ;
- être présidé par un administrateur indépendant, qui ne soit pas le président du conseil d'administration ni d'un autre comité au sein de la banque ;
- être exclusivement composé d'administrateurs non dirigeants ou indépendants ;
- compter des membres qui disposent d'une expérience dans le domaine de l'audit, de l'information financière et de la comptabilité.

[18] Voir Comité de Bâle sur le contrôle bancaire, *External audits of banks*, mars 2014, www.bis.org/publ/bcbs280.pdf.

69. Il incombe au comité d'audit de :

- définir, entre autres, les politiques d'audit interne et d'information financière ;
- surveiller le processus d'établissement des rapports financiers ;
- assurer la surveillance des auditeurs internes et externes et être leur interlocuteur ;
- approuver, ou recommander au conseil d'administration ou aux actionnaires pour approbation, la nomination[19], la rémunération et la révocation des auditeurs externes ;
- réexaminer et approuver le périmètre et la fréquence des audits ;
- être destinataire des principaux rapports d'audit et s'assurer que la direction adopte sans délai des mesures pour remédier aux insuffisances en matière de contrôles, sanctionner le non-respect des politiques, lois et règlements, et résoudre tout autre problème décelé par les auditeurs et les autres fonctions de contrôle ;
- surveiller la mise en place des principes et pratiques comptables par la banque ;
- étudier les avis des tierces parties sur la conception et l'efficacité du cadre général de gouvernance du risque et du système de contrôles internes.

70. Au minimum, les membres du comité d'audit doivent collectivement posséder une combinaison équilibrée de compétences et d'expertise – adaptée à la complexité de la banque et au mandat du comité – ainsi qu'une expérience pertinente dans les domaines de la communication financière, de la comptabilité et de l'audit. Si nécessaire, le comité d'audit peut consulter librement des experts extérieurs.

Comité de gestion des risques

71. Un comité de gestion des risques doit :

- être obligatoire dans toute banque d'importance systémique ; pour les autres banques, il est fortement recommandé, selon la taille, le profil de risque et la complexité de la banque ;
- être distinct du comité d'audit, bien que les deux comités puissent travailler sur des sujets communs, d'ordre financier par exemple ;
- être présidé par un administrateur indépendant, qui ne soit pas le président du conseil d'administration ni d'un autre comité au sein de la banque ;
- compter une majorité d'administrateurs indépendants ;
- inclure des membres ayant une expérience des questions et pratiques de gestion des risques ;
- examiner toutes les stratégies en matière de risque sur une base agrégée ainsi que par type de risque, et formuler des recommandations à l'intention du conseil à ce sujet et concernant l'appétence pour le risque ;
- passer en revue les politiques de risque de la banque au moins une fois par an ;
- veiller à ce que la direction mette en place des processus encourageant la banque à respecter les politiques de risque établies.

72. Le comité de gestion des risques fournit au conseil d'administration des avis consultatifs sur l'appétence pour le risque actuelle et future, surveille la mise en œuvre, par la direction, de la déclaration

[19] Dans certaines juridictions, les auditeurs externes sont nommés directement par les actionnaires, le conseil d'administration se contentant de formuler des recommandations.

d'appétence pour le risque, rend compte de la culture du risque dans la banque, et est l'interlocuteur du directeur de la gestion des risques, dont il assure aussi la surveillance.

73. Le comité est notamment chargé de surveiller les stratégies de gestion de la liquidité et des fonds propres, mais aussi les stratégies relatives à tous les risques auxquels la banque est exposée, comme les risques opérationnels, de crédit, de marché et de réputation, afin de s'assurer de leur cohérence avec l'appétence pour le risque telle qu'établie.

74. Le comité doit régulièrement recevoir des rapports et des informations de la part du directeur de la gestion des risques et d'autres fonctions pertinentes sur le profil de risque actuel de la banque, l'état actuel de la culture du risque, le degré d'utilisation de l'appétence pour le risque autorisée, les plafonds de risque, les dépassements de ces plafonds et les plans d'atténuation (voir Principe 6).

75. Le comité d'audit et le comité des risques doivent communiquer et collaborer efficacement afin de faciliter l'échange d'informations et la couverture effective de tous les risques, y compris émergents, ainsi que l'adoption d'ajustements du dispositif de gouvernance du risque éventuellement nécessaires.

Comité des rémunérations

76. Toutes les banques d'importance systémique doivent disposer d'un comité des rémunérations. Celui-ci doit assister le conseil d'administration dans deux de ses attributions : d'une part, surveiller l'élaboration et la mise en œuvre du système de rémunération et, d'autre part, veiller à ce que ce système soit approprié, qu'il corresponde à la culture, à l'appétence pour le risque et aux activités à long terme, à la performance et au système de contrôles de la banque (Principe 10), et qu'il soit conforme à toute exigence légale ou réglementaire. La composition du comité des rémunérations doit lui permettre d'exercer un jugement compétent et indépendant sur les politiques et les pratiques de rémunération et les incitations qui en découlent. Le comité des rémunérations travaille en étroite collaboration avec le comité des risques à l'évaluation des incitations créées par le système de rémunération. Sans préjudice des tâches confiées au comité des rémunérations, le comité des risques doit déterminer si les incitations générées par le système de rémunérations tiennent dûment compte des risques, des fonds propres, de la liquidité ainsi que de la probabilité de gains et du moment de leur obtention.

Autres comités du conseil d'administration

77. Le Comité de Bâle recommande également l'instauration d'autres comités spécialisés :

- Le *Comité des nominations ou des ressources humaines ou de gouvernance* recommande au conseil d'administration de nouveaux membres pour le conseil d'administration et la direction. Le comité des nominations doit analyser le rôle et les responsabilités du membre du conseil en question, ainsi que les connaissances, l'expérience et les compétences que le poste suppose. Même lorsque le conseil de surveillance ou le conseil d'administration est distinct de l'organe de direction, il reste nécessaire de veiller à l'objectivité et à l'indépendance du conseil par une sélection adéquate de ses membres. Le comité des nominations doit déployer tous les efforts nécessaires pour éviter qu'une seule personne ou un petit groupe de personnes ne domine le conseil d'administration au détriment des intérêts de la banque dans son ensemble. Il peut participer à l'évaluation de l'efficacité du conseil d'administration et de la direction ainsi qu'à la surveillance des politiques de la banque en matière de ressources humaines (Principe 2).
- Le *comité d'éthique et de conformité* veille à ce que la banque dispose des moyens requis afin que la prise de décision soit adéquate, que les risques d'atteinte à la réputation de la banque soient dûment pris en considération et que la législation, la réglementation et les règles internes soient respectées.

78. Le conseil doit nommer, pour siéger dans les comités spécialisés, des membres qui présentent, collectivement, une bonne combinaison de compétences et d'expérience afin que ces comités soient à même de comprendre parfaitement les questions traitées, de les examiner en toute objectivité et d'apporter de nouvelles idées.

79. Dans les juridictions qui permettent ou qui exigent que des administrateurs dirigeants siègent au conseil d'administration, le conseil d'administration doit faire en sorte que chaque comité dispose de l'objectivité nécessaire à ses attributions, par exemple en décidant que les comités seront composés uniquement d'administrateurs non dirigeants ou, si possible, d'une majorité d'administrateurs indépendants.

Conflits d'intérêts

80. Des conflits d'intérêts peuvent naître de la pluralité des activités et des rôles de la banque (par exemple, lorsqu'elle octroie des prêts à une entreprise alors que sa fonction de négoce pour compte propre achète et vend des titres émis par cette entreprise), ou d'une contradiction entre les intérêts de la banque ou de ses clients et ceux des membres du conseil d'administration ou de la direction (par exemple, si la banque entre en relation d'affaires avec une entité dans laquelle l'un des administrateurs de la banque a un intérêt financier).

81. Des conflits d'intérêts peuvent aussi survenir lorsqu'une banque fait partie d'un groupe. Ainsi, les circuits hiérarchiques et les flux d'informations entre la banque, sa société mère et d'autres filiales peuvent donner lieu à des conflits d'intérêts (par exemple, le partage d'informations exclusives, confidentielles ou sensibles, ou des pressions visant à mener des transactions à des conditions non concurrentielles).

82. Le conseil d'administration doit surveiller la mise en œuvre des politiques visant à détecter d'éventuels conflits d'intérêts. Lorsqu'ils ne peuvent être prévenus, ces conflits doivent être convenablement gérés (certaines relations ou transactions sont tolérées dans le cadre de saines politiques d'entreprise, conformes à la législation nationale et aux normes prudentielles).

83. Le conseil d'administration doit mettre en place une politique officielle relative aux conflits d'intérêts, sous forme écrite, et un processus objectif de contrôle de la conformité avec cette politique. Cette politique doit prévoir :

- l'obligation pour un membre d'éviter, dans la mesure du possible, de mener toute activité qui pourrait donner lieu à un conflit d'intérêts, apparent ou avéré ;
- des exemples de conflits susceptibles de se présenter à un membre du conseil d'administration ;
- un examen et un processus d'approbation rigoureux qui s'appliquent aux membres du conseil avant qu'ils s'engagent dans certaines activités (comme le fait de siéger dans un autre conseil d'administration), afin que ces activités ne créent pas de conflits d'intérêts[20] ;
- l'obligation pour un membre de signaler rapidement tout élément qui pourrait donner ou aurait donné lieu à un conflit d'intérêts ;
- l'engagement des membres à s'abstenir de voter sur des questions pour lesquelles ils pourraient être en situation de conflit d'intérêts ou lorsque leur objectivité ou leur capacité à remplir correctement leurs obligations envers la banque pourraient se trouver compromises ;

[20] Ce type d'examen pourrait, par exemple, être effectué par au moins deux membres du conseil ou par un comité du conseil, ou avec la participation de la fonction gestion des risques, conformité ou audit interne, ou encore en collaboration avec un expert externe indépendant.

- des procédures qui encadrent de façon adéquate les transactions avec des parties liées afin qu'elles respectent les conditions de pleine concurrence ;
- la manière dont le conseil traitera les cas de non-respect de cette politique.

84. Dans le cadre des politiques de gestion des conflits d'intérêts et en cas d'éventuels conflits d'intérêts importants, le conseil d'administration doit surveiller le processus d'information du public et des autorités de contrôle, et établir qu'il est approprié.

85. Cette surveillance doit également porter sur les informations relatives à l'approche de la banque eu égard à la divulgation et à la gestion des conflits d'intérêts importants qui sont en contradiction avec ces politiques, ainsi que des conflits qui pourraient résulter de l'appartenance de la banque à un groupe bancaire ou de transactions avec d'autres entités au sein d'un groupe bancaire.

86. Un conflit d'intérêts peut apparaître lorsqu'une banque est la propriété d'un État qui exerce également le contrôle bancaire. Si ce conflit d'intérêts est avéré, les fonctions de propriétaire et celles d'autorité de contrôle bancaire doivent être exercées par deux administrations totalement distinctes afin de limiter le plus possible les interférences politiques dans la supervision de la banque.

Principe 4 – Direction

Placée sous l'autorité et la surveillance du conseil d'administration, la direction doit assurer l'exécution et la gestion des activités de la banque conformément à la stratégie opérationnelle, à l'appétence pour le risque, à la politique de rémunération et aux autres politiques approuvées par le conseil.

87. La direction est un groupe restreint de personnes clés, chargé d'assurer la gestion courante, saine et prudente des activités de la banque. Elle rend compte au conseil d'administration.

88. La structure et les procédures de la direction, notamment en matière de prise de décision, doivent être claires et transparentes, et de nature à favoriser une gestion efficace de la banque. Ainsi, le rôle, les pouvoirs et les responsabilités qui s'attachent aux différents postes de direction, dont celui de directeur général, doivent être clairement définis.

89. Les membres de la direction doivent disposer de l'expérience, des compétences et de l'intégrité nécessaires à la gestion des activités de la banque et des agents placés sous leurs ordres. Ils doivent recevoir une formation régulière afin de conserver et d'approfondir leurs compétences et de se tenir à jour des connaissances dans leurs domaines de responsabilité.

90. Les membres de la direction doivent être choisis à l'issue d'un processus de recrutement ou de promotion adéquat, qui prenne en compte les qualifications requises pour le poste. Pour les postes de direction soumis à un examen ou une sélection par le conseil d'administration après un entretien avec les candidats, la direction doit lui communiquer les informations dont il a besoin.

91. La direction contribue de façon substantielle à la bonne gouvernance de la banque par sa conduite (c'est-à-dire en montrant l'exemple de même que le conseil d'administration). Les membres de la direction doivent assurer une surveillance adéquate de leurs collaborateurs, veiller à ce que les activités de la banque soient conformes à la stratégie établie, à l'appétence pour le risque et aux politiques approuvées par le conseil d'administration.

92. La direction est chargée de déléguer des tâches aux employés et d'établir une structure de gestion qui incite l'ensemble de la banque à faire preuve de responsabilité et de transparence.

93. Conformément aux orientations données par le conseil d'administration, la direction doit appliquer les stratégies opérationnelles, les systèmes de gestion des risques, la culture du risque mais aussi les processus et les contrôles permettant de gérer les risques (de nature financière ou non) auxquels elle est exposée et concernant lesquels elle est tenue de respecter les lois, les règlements et les politiques internes.

- Cela suppose l'existence de fonctions gestion des risques, conformité et audit qui soient indépendantes et dotées d'un large mandat, ainsi que d'un système général de contrôles internes efficace. La direction doit reconnaître et respecter l'indépendance de ces fonctions et se garder d'interférer dans l'accomplissement de leurs tâches.

94. La direction doit communiquer au conseil d'administration les informations dont il a besoin pour exercer ses responsabilités, superviser la direction et en évaluer les performances. À cet égard, la direction doit, de façon régulière et adéquate, tenir le conseil d'administration informé de sujets importants, tels que :

- les changements dans la stratégie opérationnelle, la stratégie en matière de risque ou d'appétence pour le risque ;
- les performances et la situation financière de la banque ;
- les dépassements des plafonds de risque et les infractions aux règles de conformité ;

- les échecs des contrôles internes ;
- les préoccupations sur des sujets ayant trait à la réglementation ou à la loi ;
- les problèmes soulevés dans le cadre de la procédure de lancement d'alerte.

Principe 5 – Gouvernance des groupes bancaires

Dans un groupe bancaire, le conseil d'administration de la société mère assume la responsabilité générale des activités du groupe. Il est chargé de définir et de mettre en œuvre un dispositif de gouvernance clair et adapté à la structure, à l'activité et aux risques du groupe et de ses entités[21]. Le conseil d'administration et la direction doivent connaître et comprendre la structure du groupe et les risques qu'elle pose.

Conseil d'administration de la société mère

95. Le conseil d'administration de la société mère opérant au sein d'une structure de groupe, il doit être conscient des principaux risques et problèmes qui peuvent toucher à la fois la banque dans son ensemble et chacune de ses filiales. Il doit exercer une surveillance adéquate des filiales tout en respectant les propres responsabilités juridiques et de gouvernance qui peuvent échoir aux conseils d'administration des filiales.

96. Afin d'exercer ses responsabilités, le conseil d'administration de la société mère doit :

- établir une structure de groupe (entité juridique et structure opérationnelle) et un cadre de gouvernance d'entreprise doté de rôles et responsabilités clairement définis, tant au niveau de la société mère que des filiales, et adaptés à la complexité et à l'importance des filiales ;
- définir une structure adéquate pour le conseil d'administration et la direction de chaque filiale, qui tienne compte des risques significatifs auxquels le groupe, ses activités et ses filiales sont exposés ;
- déterminer si le cadre de gouvernance du groupe comprend des politiques, des processus et des contrôles adéquats, et si ledit cadre organise la gestion des risques pour l'ensemble des activités et entités juridiques ;
- veiller à ce que le cadre de gouvernance du groupe prévoie des processus et des contrôles appropriés pour détecter et gérer les conflits d'intérêts potentiels à l'intérieur du groupe, résultant notamment des transactions intragroupe ;
- approuver des politiques et des stratégies claires quant à la création de nouvelles structures et entités juridiques et veiller à ce qu'elles soient cohérentes avec les politiques et les intérêts du groupe ;
- vérifier qu'il existe des systèmes efficaces pour faciliter la communication d'informations entre les différentes entités, gérer les risques des différentes filiales ou entités du groupe, mais aussi du groupe dans son ensemble, et permettre une supervision efficace du groupe ;
- disposer des ressources suffisantes pour vérifier la conformité des filiales avec l'ensemble des exigences applicables en matière de gouvernance, lois et règlements ;

[21] Les banques faisant partie d'un conglomérat doivent également tenir compte des principes de contrôle des conglomérats financiers rédigés par l'Instance conjointe (*Principles for the supervision of financial conglomerates*, septembre 2013, www.bis.org/publ/joint29.htm). Dans le présent document, les termes « société mère » et « groupe » s'appliquent à un groupe financier.

- entretenir une relation efficace avec l'autorité de contrôle du pays du siège et avec l'autorité de contrôle de chaque filiale, directement ou par le biais du conseil d'administration ;
- établir une fonction d'audit interne qui veille à ce que des audits soient réalisés dans chaque filiale ou pour l'ensemble d'entre elles et pour chaque partie du groupe et pour le groupe dans son ensemble[22] ;
- veiller à ce que le cadre de gouvernance du groupe prévoie des processus et des contrôles appropriés pour détecter et gérer les conflits d'intérêts potentiels à l'intérieur du groupe, résultant notamment des transactions intragroupe, en tenant dûment compte des intérêts du groupe.

Conseil d'administration d'une filiale[23]

97. Le conseil d'administration et la direction de chaque filiale restent responsables de l'élaboration d'un processus de gestion des risques efficace pour l'entité qui leur incombe. Les méthodes et les procédures en vigueur dans les filiales doivent concourir à l'efficacité de la gestion des risques à l'échelle du groupe. La société mère est chargée de la gestion stratégique des risques à l'échelle du groupe et de la définition des politiques de risque applicables, mais ce sont le conseil d'administration et la direction de chaque filiale qui déterminent de façon adéquate la mise en œuvre de cette gestion et de ces politiques au niveau local et régional ainsi que l'évaluation des risques à l'échelle locale. La société mère doit veiller à ce que chaque filiale dispose des outils et de l'autorité nécessaires, et à ce qu'elle comprenne ses obligations de rendre compte au siège. Le conseil d'administration de chaque filiale doit s'assurer que les politiques du groupe sont compatibles avec les obligations légales et réglementaires locales et, le cas échéant, modifier ces politiques.

98. Les objectifs stratégiques, le cadre de gouvernance du risque, le système de valeurs et les principes de gouvernance de la filiale doivent être conformes à ceux de la société mère (ci-après les « politiques du groupe »), mais la filiale doit procéder aux ajustements nécessaires lorsqu'une politique du groupe est en contradiction avec une disposition légale, réglementaire ou prudentielle, ou lorsqu'elle serait préjudiciable à la gestion saine et prudente de la filiale.

99. Dans le cas d'une filiale importante soumise à réglementation (du fait de son profil de risque, de son importance systémique ou de sa taille par rapport à celle de la société mère), le conseil d'administration de cette filiale doit prendre les mesures supplémentaires qui sont nécessaires pour que la filiale puisse exercer ses propres responsabilités en matière de gouvernance d'entreprise et respecter les exigences légales et réglementaires qui s'appliquent à elle.

Structures complexes ou opaques

100. Les banques créent des structures à des fins légales, réglementaires ou fiscales. Ces structures peuvent prendre la forme d'unités, de succursales, de filiales ou autres entités juridiques, et accroître considérablement le degré de complexité de l'organisation. Le nombre de ces entités et en particulier leurs interactions et leurs transactions intragroupes peuvent rendre difficiles la détection et la gestion des risques à l'échelle de l'organisation.

[22] Voir Comité de Bâle sur le contrôle bancaire, *Internal audit function in banks*, www.bis.org/publ/bcbs223.pdf.

[23] Voir aussi paragraphe 123.

101. Lorsqu'une banque opère au travers de structures complexes ou opaques, elle s'expose à des risques financiers, juridiques ou de réputation. Ce type de fonctionnement peut empêcher le conseil d'administration et la direction d'exercer une surveillance adéquate, et nuire à l'efficacité du contrôle bancaire[24].

102. La direction et, le cas échéant, le conseil d'administration doivent être conscients de ces risques et s'efforcer de les éviter ou de les atténuer en :

- évitant d'instaurer des structures complexes sans substance économique ou but opérationnel ;
- veillant au maintien et à l'examen constants de la pertinence des politiques, des procédures et des processus régissant l'approbation et la conservation de ces structures ou de ces activités, notamment par la vérification rigoureuse de leur objet, des risques associés et de la capacité de la banque à gérer ces risques, avant de créer de nouvelles structures et de lancer les activités associées ;
- appliquant un processus centralisé d'approbation pour la création de nouvelles entités juridiques ou de filiales sur la base de critères préalablement établis ; il doit notamment pouvoir suivre, pour chaque entité, le respect des obligations en matière de réglementation, d'imposition, d'information financière et de gouvernance, et être en mesure de dissoudre les filiales en sommeil ;
- établissant des procédures et processus adéquats pour détecter et gérer tous les risques importants émanant de ces structures, tels que le manque de transparence de la gestion, les risques opérationnels nés de l'interaction et de la complexité des structures de financement, les expositions intragroupe, les sûretés immobilisées et le risque de contrepartie. Seules les structures dont les risques importants ont pu être convenablement détectés, évalués et gérés doivent être approuvées par la banque ;
- vérifiant que les activités et la structure de la banque font l'objet d'audits internes et externes réguliers.

103. Le conseil d'administration de la société mère peut renforcer l'efficacité des efforts susmentionnés en imposant un examen officiel, indépendant et périodique de ces structures, de leurs processus de contrôle et de leurs activités, ainsi que de leur concordance avec la stratégie approuvée par le conseil d'administration.

104. Le conseil d'administration doit se tenir prêt à examiner, avec les autorités de contrôle de la banque et du pays d'accueil, les politiques et stratégies adoptées eu égard à la création et au maintien de ces structures et activités et, si nécessaire, à leur en rendre compte.

[24] En outre, la banque peut être exposée à des risques indirects lorsqu'elle offre certains services ou met en place des structures pour le compte de sa clientèle. Voir Comité de Bâle sur le contrôle bancaire, *Devoir de diligence des banques au sujet de la clientèle*, octobre 2001, www.bis.org/publ/bcbs85f.pdf. Il peut s'agir par exemple de servir d'agent dans la constitution d'entreprises ou de partenariats, de fournir divers services de mandataire ou de monter des transactions complexes de finance structurée au bénéfice de clients. Ces prestations sont souvent lucratives et peuvent servir les buts professionnels légitimes de la clientèle, mais il peut arriver que ces produits et activités proposés par les banques soient utilisés à des fins illicites ou inappropriées par les clients.

Principe 6 – Fonction gestion des risques

Il doit exister dans chaque banque une fonction gestion des risques indépendante et efficace, placée sous la responsabilité d'un directeur de la gestion des risques doté de la stature, de l'indépendance et des ressources nécessaires et ayant accès au conseil d'administration.

105. Une fonction gestion des risques indépendante est un élément clé de la deuxième ligne de défense de la banque. Cette fonction est chargée de surveiller toute activité comportant une prise de risque et elle doit disposer, au sein de l'organisation, de l'autorité nécessaire pour ce faire. La fonction gestion des risques doit principalement :

- détecter les risques importants et les risques émergents, pris individuellement et à l'échelle globale ;
- évaluer ces risques et le niveau d'exposition de la banque à ces risques ;
- sous réserve de l'examen et de l'approbation du conseil d'administration, élaborer et mettre en œuvre le cadre de gouvernance du risque à l'échelle de la banque, y compris culture du risque, appétence pour le risque et plafonds de risque ;
- exercer un suivi permanent des activités comportant une prise de risque et des expositions au risque, compte tenu de l'appétence pour le risque, des plafonds de risque et des besoins de fonds propres ou de liquidité qui en découlent (c'est-à-dire planification des fonds propres), tels qu'approuvés par le conseil d'administration ;
- instaurer un système de détection ou d'alerte précoce en cas d'infraction à l'appétence pour le risque ou de dépassement des plafonds de risque de la banque ;
- orienter, voire remettre en question, les décisions qui donnent lieu à des risques importants ;
- rendre compte à la direction et au conseil d'administration, ou à son comité des risques, de toutes ces questions et, notamment, proposer des mesures adéquates pour atténuer ces risques.

106. S'il est d'usage que la fonction gestion des risques collabore étroitement avec les départements opérationnels, elle doit cependant être suffisamment indépendante de ces départements et s'abstenir de participer à toute production de revenus. Cette indépendance est une caractéristique essentielle d'une fonction gestion des risques efficace, de même que la liberté d'entrer en relation avec toutes les unités opérationnelles qui peuvent générer des risques importants pour la banque ainsi qu'avec les filiales et établissements affiliés qui présentent des risques.

107. La fonction gestion des risques doit compter un nombre suffisant d'employés qui disposent de l'expérience et des qualifications requises, en particulier d'une bonne connaissance du marché et des produits et d'une excellente maîtrise des différents aspects de la gestion des risques[25]. Les employés doivent être capables et désireux de remettre en question des opérations de la banque, eu égard à tous les aspects des risques résultant des activités. Les employés doivent avoir régulièrement accès à une formation.

Rôle du directeur de la gestion des risques

108. Dans les banques de grande envergure, complexes et ayant des activités internationales, mais aussi dans d'autres banques, selon leur profil de risque et les exigences locales de gouvernance, le

[25] Certaines banques estiment qu'une bonne pratique consiste à encourager ou obliger les employés à enrichir leur expérience en alternant les postes dans les départements opérationnels et dans la gestion des risques. Cette approche peut présenter de nombreux avantages : elle permet notamment de conférer à la gestion des risques un poids comparable à celui des départements opérationnels et autres fonctions, de promouvoir un dialogue sur le risque à l'échelle de la banque et de faire comprendre aux opérationnels l'importance de la gestion des risques et aux gestionnaires des risques, le fonctionnement des départements opérationnels. Toutefois, afin d'éviter les conflits d'intérêts, les gestionnaires des risques ne doivent pas être chargés du contrôle d'activités dont ils ont été directement responsables ou pour lesquelles ils ont participé à la prise de décision ou au processus d'approbation.

responsable de la fonction gestion des risques doit être un cadre dirigeant (directeur de la gestion des risques ou équivalent). Les groupes bancaires doivent non seulement disposer d'un directeur de la gestion des risques pour l'ensemble du groupe, mais aussi d'un responsable des risques dans chaque filiale. Dans certaines banques, le poste de responsable de la gestion des risques peut s'intituler différemment, mais dans le présent document « directeur de la gestion des risques » renvoie à tout poste équivalent, sous réserve qu'il respecte les critères décrits ici, en particulier en matière d'indépendance.

109. Le directeur de la gestion des risques a pour principale mission de surveiller l'élaboration et la mise en œuvre de la fonction gestion des risques. Il lui incombe donc de renforcer constamment les compétences de ses équipes et d'améliorer les systèmes, les politiques, les processus, les modèles quantitatifs et les rapports relatifs à la gestion des risques, de façon à ce que la banque dispose de capacités de gestion des risques suffisamment solides et efficaces pour servir correctement ses objectifs stratégiques et la totalité de ses activités à risque. Il est également chargé d'apporter son assistance au conseil d'administration lorsqu'il détermine et surveille l'appétence pour le risque et la déclaration y afférente, et qu'il traduit l'appétence pour le risque en plafonds de risque. Conjointement avec la direction, le directeur de la gestion des risques doit participer activement au suivi des performances en matière de risque et de respect des plafonds. Il doit également gérer des processus de prise de décision clés et y participer (planification stratégique, des fonds propres et de la liquidité, nouveaux produits et services, élaboration et mise en œuvre du système de rémunération).

110. Le directeur de la gestion des risques doit disposer, au sein de l'organisation, de la stature, de l'autorité et des compétences nécessaires pour surveiller les activités de gestion des risques de la banque. Il doit être indépendant et ses obligations doivent être distinctes de celles d'autres fonctions exécutives. Le directeur de la gestion des risques doit avoir accès à toutes les informations nécessaires pour accomplir les tâches qui lui incombent. Toutefois, il ne doit exercer aucune fonction financière ou de gestion en rapport avec un département opérationnel ou une fonction génératrice de revenus, ni cumuler ses attributions avec un autre poste clé (directeur des opérations, directeur financier, chef de l'audit, ou autre poste de dirigeant)[26]. Si les structures hiérarchiques peuvent varier d'une banque à l'autre, le directeur de la gestion des risques doit toujours rendre compte au conseil d'administration et avoir librement accès au conseil ou à son comité des risques. Le directeur de la gestion des risques doit être capable d'interpréter et de formuler les risques de façon claire et compréhensible et d'engager un dialogue constructif avec le conseil d'administration et la direction sur des questions essentielles en matière de risque. Le directeur de la gestion des risques doit régulièrement interagir avec le conseil d'administration ou son comité des risques, et il doit pouvoir se réunir avec eux en l'absence d'administrateurs dirigeants[27].

111. La nomination et la révocation du directeur de la gestion des risques ainsi que tout autre changement relatif à ce poste doivent être approuvés par le conseil d'administration ou par son comité des risques. Lorsque le directeur de la gestion des risques est démis de ses fonctions, cette information doit être rendue publique, et la banque doit justifier de cette décision auprès de son autorité de contrôle. Les performances et la rémunération du directeur de la gestion des risques, tout comme le budget qui lui est alloué, doivent être évalués et approuvés par le conseil d'administration ou son comité des risques.

[26] Lorsqu'un tel cumul est inévitable (comme dans les petits établissements, du fait de ressources limitées), ces rôles doivent être compatibles (ainsi, le directeur de la gestion des risques pourrait être aussi responsable d'un domaine de risque particulier) et ils ne doivent pas mettre en péril l'équilibre des pouvoirs.

[27] Il arrive que le directeur de la gestion des risques siège au comité de crédit, dont la mission est d'approuver les expositions sur prêts. Si la participation du directeur de la gestion des risques peut améliorer la prise de décision, et s'avérer également utile au directeur lui-même – qui s'informe ainsi des expositions éventuelles (et des pratiques d'octroi de prêt) à prendre en compte dans le processus de suivi des prêts –, elle peut néanmoins le placer en situation de conflit s'il est amené, par la suite, à signaler ou critiquer une exposition. Certaines banques estiment que, dans de tels cas, il vaut mieux que le directeur ne dispose que d'un pouvoir de veto (et non d'un pouvoir d'approbation).

Principe 7 – Détection, suivi et contrôle des risques

Il convient de détecter, suivre et contrôler les risques de façon régulière au niveau du groupe et de chacune de ses entités. Le degré de complexité des structures de gestion des risques et de contrôle interne de la banque doit s'adapter à l'évolution du profil de risque de la banque, des risques extérieurs et des pratiques du secteur.

112. Le dispositif de gouvernance du risque doit inclure des politiques, reposant sur des procédures et processus de contrôle appropriés, qui garantissent que les capacités de la banque à détecter, agréger, atténuer et suivre les risques soient en adéquation avec sa taille, sa complexité et son profil de risque.

113. La détection des risques doit porter sur tous les risques, au bilan ou hors bilan, importants pour la banque, qu'ils se situent au niveau du groupe, de chaque portefeuille ou de chaque unité opérationnelle. Afin d'évaluer efficacement les risques, le conseil d'administration et la direction, dont le directeur de la gestion des risques, doivent procéder à une estimation aussi bien régulière que ponctuelle des risques et du profil de risque général de la banque. Cette évaluation doit comprendre une analyse systématique des risques existants et la détection des nouveaux risques émergents et ce, pour toutes les unités de l'organisation. Les concentrations associées à des risques importants doivent également être prises en considération dans l'évaluation des risques.

114. La détection et l'évaluation des risques doivent porter sur des éléments à la fois quantitatifs et qualitatifs. L'évaluation doit aussi s'appuyer sur l'opinion qualitative, à l'échelle de la banque, à l'égard des risques liés à l'environnement opérationnel extérieur à la banque. Les banques doivent également prendre en considération et évaluer les risques difficiles à mesurer, comme le risque de réputation.

115. Le système de contrôles internes est notamment conçu pour vérifier qu'à chaque risque majeur est associé une politique, un processus ou un autre outil, ainsi qu'un dispositif destiné à contrôler la mise en œuvre et le bon fonctionnement de ces outils. Il permet ainsi d'assurer l'intégrité, la conformité et l'efficacité des processus. De plus, il donne l'assurance raisonnable que les données financières et de gestion sont fiables, à jour et exhaustives, et que la banque est en conformité avec ses différentes politiques ainsi qu'avec les lois et règlements applicables.

116. Afin de prévenir toute action outrepassant les pouvoirs attachés à une fonction, voire la fraude, le système de contrôles internes fixe, pour la direction et le personnel, des limites raisonnables à l'exercice de leurs pouvoirs de discrétion. Ainsi, même dans les petites banques, les décisions de gestion importantes ne doivent pas reposer sur une seule personne. En outre, des examens internes doivent déterminer dans quelle mesure une banque respecte ses propres politiques et procédures ainsi que les lois et règlements en vigueur. Des procédures adéquates d'alerte des niveaux hiérarchiques supérieurs constituent un élément clé du système de contrôles internes.

117. Le degré de complexité de l'infrastructure de gestion des risques de la banque – dont, en particulier, une infrastructure et une architecture des données ainsi qu'une infrastructure informatique suffisamment solides – doit évoluer en suivant : la croissance du bilan et des revenus ; l'augmentation de la complexité des activités, de la configuration des risques et de la structure opérationnelle de la banque ; l'expansion géographique ; les fusions-acquisitions ; et l'adoption de nouveaux produits ou lignes de métier.

118. Les banques doivent disposer de données internes et externes exactes pour détecter, évaluer et atténuer les risques, prendre des décisions opérationnelles stratégiques et déterminer l'adéquation des fonds propres et de la liquidité. Le conseil d'administration et la direction doivent accorder une importance particulière à la qualité, à l'exhaustivité et à l'exactitude des données qui étayent leurs décisions en matière

de risque[28]. Si le recours aux notations externes ou à des modèles de risque et des données acquis auprès de fournisseurs extérieurs peut s'avérer utile pour mener une évaluation plus approfondie, les banques restent responsables en dernier ressort de leur évaluation des risques.

119. L'évaluation des risques et les techniques de modélisation doivent compléter l'analyse et le suivi qualitatifs des risques, et non s'y substituer. La fonction gestion des risques doit informer le conseil et la direction des hypothèses et des éventuelles lacunes des modèles et analyses de risque utilisés par la banque, afin d'améliorer la compréhension des risques et des expositions, et de permettre, le cas échéant, une intervention plus rapide pour gérer et atténuer les risques.

120. Dans le cadre de ses analyses quantitatives et qualitatives, la banque doit recourir à des tests de résistance et à des analyses de scénarios de crise afin de mieux comprendre les expositions au risque potentielles dans différentes situations défavorables[29] :

- les tests de résistance internes doivent couvrir un ensemble de scénarios fondés sur des hypothèses raisonnables en matière de dépendances et de corrélations. La direction doit définir et approuver les scénarios utilisés dans les analyses de risque de la banque et, le cas échéant, le conseil d'administration doit les examiner d'un œil critique ;
- des tests de résistance inversés peuvent fournir des informations supplémentaires sur la position de la banque à l'égard du risque et sur des décisions de gestion qui pourraient être prises à l'avenir ;
- les résultats des tests de résistance doivent être régulièrement examinés avec le conseil ou son comité des risques. Ces résultats doivent être pris en compte dans l'examen de l'appétence pour le risque, du processus d'évaluation de l'adéquation des fonds propres, de la planification des fonds propres et de la liquidité, et des budgets. Ils doivent également être mis en lien avec les plans de redressement et de résolution. La fonction gestion des risques doit, le cas échéant, proposer les actions nécessaires à la lumière de ces résultats ;
- les résultats des tests de résistance et des analyses de scénarios de crise doivent également être communiqués aux unités opérationnelles et aux personnes concernées, qui doivent en tenir dûment compte.

121. Les banques doivent régulièrement comparer les performances effectives au regard des risques estimés (contrôles *ex post*), ce qui permet d'évaluer la précision et l'efficacité du processus de gestion des risques et d'apporter les changements nécessaires.

122. La fonction gestion des risques doit non seulement détecter et mesurer les expositions aux risques, mais aussi envisager les moyens de les atténuer. Dans certains cas, la fonction gestion des risques peut ordonner la réduction ou la couverture des risques afin de limiter l'exposition. Dans d'autres cas, par exemple lorsque la banque accepte ou décide de prendre des risques supérieurs aux plafonds définis (de façon temporaire) ou d'assumer des risques qui ne peuvent pas être couverts ou atténués, la fonction gestion des risques doit informer le conseil d'administration des exemptions importantes et suivre ces positions pour s'assurer qu'elles restent dans le cadre des contrôles et plafonds fixés par la banque ou dans les limites d'approbation des exceptions. Chacune de ces approches peut s'avérer pertinente selon

[28] Voir Comité de Bâle sur le contrôle bancaire, *Principes aux fins de l'agrégation des données sur les risques et de la notification des risques*, janvier 2013, et son rapport intermédiaire de janvier 2015.

[29] Voir Comité de Bâle sur le contrôle bancaire, *Principles for sound stress testing practices and supervision*, mai 2009, www.bis.org/publ/bcbs155.htm.

la situation qui se présente, à condition que l'indépendance de la fonction gestion des risques ne soit pas compromise.

123. Les banques doivent disposer de processus de gestion des risques et d'approbation en ce qui concerne la création et l'expansion de produits, services, activités et marchés, ainsi que les grosses transactions complexes qui absorbent beaucoup de ressources ou qui présentent des risques difficiles à mesurer. Les banques doivent également disposer de processus d'examen et d'approbation pour l'externalisation des fonctions bancaires[30]. La fonction gestion des risques doit apporter des informations sur les risques dans le cadre de ces processus et sur la capacité du fournisseur externe à gérer les risques et à respecter les obligations légales et réglementaires. Ces processus doivent comprendre :

- une évaluation complète et franche des risques dans divers scénarios ainsi que de l'incapacité potentielle de la gestion des risques et des contrôles internes à gérer efficacement les risques associés ;
- une appréciation de la mesure dans laquelle les départements chargés de la gestion des risques, de la conformité légale et réglementaire, des technologies de l'information, des activités opérationnelles et des contrôles internes disposent des outils et de l'expertise nécessaires pour mesurer et gérer les risques en question.

En l'absence de processus adéquat de gestion des risques, la mise en place de tout nouveau produit, service, activité, relation avec une partie tierce ou transaction majeure doit être reportée jusqu'à ce que la banque soit en mesure de bien gérer cette nouvelle activité. Il doit également y avoir un processus d'évaluation des risques et de la performance au regard des projections initiales, et d'adaptation de la gestion des risques au fur et à mesure que la banque se développe.

124. Des mécanismes de détection et d'évaluation des risques sont également nécessaires dans les filiales et les établissements affiliés[31]. Les filiales et établissements affiliés importants et générateurs de risques doivent être pris en compte dans le système de gestion des risques à l'échelle de la banque et intégrés au cadre de gouvernance du risque[32].

125. Les fusions et acquisitions, les cessions et tout autre changement dans la structure de la banque peuvent présenter des difficultés particulières en matière de gestion des risques. En particulier, des risques peuvent surgir lorsque les vérifications requises sont appliquées mais ne parviennent pas à détecter les risques postérieurement à la fusion, ou bien en raison d'activités qui entrent en conflit avec les objectifs stratégiques de la banque ou avec son appétence pour le risque. La fonction gestion des risques doit participer activement à l'évaluation des risques qui peuvent découler de fusions ou d'acquisitions, et informer le conseil et la direction de ses conclusions.

30 Voir Instance conjointe, *Outsourcing in financial services*, www.bis.org/publ/joint12.pdf.

31 Toutefois, la législation nationale peut exempter les filiales de certaines exigences prudentielles, sur base autonome, si elles sont bien intégrées dans un groupe et satisfont à un certain nombre de conditions préalables. Les considérations énoncées dans ce paragraphe sont valables en l'absence de telles exemptions.

32 Le dispositif de gouvernance du risque doit également couvrir les établissements affiliés générateurs de risques importants afin que les politiques, les stratégies opérationnelles, les processus et les contrôles des établissements affiliés soient globalement alignés sur les objectifs du groupe.

Principe 8 – Communication en matière de risque

Un dispositif de gouvernance du risque efficace suppose une bonne communication sur les risques, tant dans les différents départements de la banque que par le biais des rapports remis au conseil d'administration et à la direction.

126. Une communication régulière destinée à l'ensemble de la banque sur les questions de risque, et notamment sur la stratégie de la banque en la matière, est l'un des piliers d'une solide culture du risque. Cette dernière doit encourager le personnel à prendre conscience des risques, à en parler librement et de façon critique, tant horizontalement dans l'organisation que verticalement, depuis et vers le conseil d'administration et la direction. La direction doit diligemment informer et consulter les fonctions de contrôle sur ses principaux plans et activités afin que ces fonctions puissent dûment s'acquitter de leurs tâches.

127. Les informations communiquées au conseil d'administration et à la direction doivent être à jour, exactes et aisément compréhensibles de façon à ce que ces organes soient en mesure de prendre des décisions éclairées. Les responsables, notamment de la fonction gestion des risques, doivent certes s'assurer que le conseil d'administration et la direction sont suffisamment informés, mais ils doivent néanmoins veiller à limiter le volume d'informations fournies, sous peine de rendre les points clés difficiles à repérer. Les informations doivent donc être hiérarchisées et présentées de façon concise et en contexte. Le conseil d'administration doit évaluer la pertinence des informations qu'il reçoit ainsi que le processus permettant d'en garantir l'exactitude, et déterminer s'il a besoin d'informations supplémentaires ou si, au contraire, il souhaite des informations plus concises.

128. Les informations *ad hoc* sur des risques significatifs qui requièrent une décision ou une réponse immédiate doivent être rapidement communiquées à la direction et, le cas échéant, au conseil d'administration, aux directeurs concernés et, éventuellement, aux chefs des fonctions de contrôle, afin que des mesures adaptées soient appliquées à un stade précoce.

129. Les rapports sur les risques soumis au conseil d'administration doivent être soigneusement conçus, afin que les risques à l'échelle de la banque, au niveau des différents portefeuilles, ou tout autre risque, soient présentés de façon concise et efficace. Ces rapports doivent fournir des informations exactes sur les expositions au risque ainsi que les résultats des tests de résistance et des analyses de scénarios. Ils doivent susciter des débats approfondis sur les expositions actuelles et attendues de la banque (en particulier en situation de tensions), sur l'équilibre entre risque et rendement, sur l'appétence pour le risque et sur les plafonds de risque, par exemple. En outre, ils doivent renseigner sur l'environnement extérieur afin de recenser les conditions et les tendances du marché qui pourraient avoir un impact sur le profil de risque actuel ou futur de la banque.

130. L'organisation des rapports sur les risques doit être dynamique, exhaustive et précise, et elle doit s'appuyer sur un ensemble d'hypothèses sous-jacentes. Le suivi des risques et les rapports à ce sujet ne doivent pas se limiter au niveau désagrégé (risques significatifs existants dans les filiales), mais porter aussi sur les risques agrégés afin de fournir une vue d'ensemble des expositions à l'échelle de la banque. Les rapports sur les risques doivent présenter clairement toute déficience ou limite dans l'estimation des risques, ainsi que toute hypothèse sous-jacente importante (interdépendance ou corrélation entre les risques, par exemple).

131. Les banques doivent éviter tout cloisonnement dans l'organisation qui soit susceptible d'entraver la bonne circulation de l'information et de conduire à des décisions prises indépendamment du reste de la banque[33]. Pour lever les obstacles à la circulation de l'information, le conseil d'administration, la direction et les fonctions de contrôle devront peut-être réévaluer les pratiques établies afin d'encourager une meilleure communication.

[33] Le cloisonnement désigne le fait que des lignes de métier, des entités juridiques ou des pôles géographiques sont gérés indépendamment les uns des autres, avec un partage limité d'informations et, dans certains cas, en concurrence les uns avec les autres.

Principe 9 – Conformité

Il incombe au conseil d'administration de surveiller la gestion du risque de non-conformité. Le conseil d'administration doit instaurer une fonction conformité et approuver les politiques et procédures de détection, d'évaluation et de suivi du risque, ainsi que celles régissant l'établissement de rapports et la fourniture de conseils à ce sujet.

132. Une fonction conformité[34] indépendante est un élément clé de la deuxième ligne de défense de la banque. Elle est notamment chargée de veiller à ce que la banque mène ses activités avec intégrité et observe les lois, réglementations et politiques internes applicables.

133. Il revient à la direction de la banque d'établir une politique de conformité qui présente les principes fondamentaux que le conseil d'administration doit approuver et qui explique les principales procédures de détection et de gestion des risques de non-conformité à chacun des niveaux de la banque.

134. Si le conseil d'administration et la direction sont responsables de la conformité des activités de la banque, la fonction conformité a un rôle important à jouer dans la promotion du système de valeurs de la banque, des politiques et procédures qui contribuent à la conduite responsable de la banque et au respect de toutes les obligations applicables.

135. La fonction conformité doit exercer un rôle de conseiller auprès du conseil d'administration et de la direction sur les questions de respect des lois, règles et normes applicables et les tenir au courant des évolutions en la matière. Elle doit également participer à la formation du personnel sur les questions de conformité, répondre à toute demande des employés sur le sujet et leur fournir des orientations sur la bonne mise en œuvre des lois, règles et normes applicables, sous la forme de politiques, procédures et autres documents tels que manuel de conformité, code de conduite et recommandations pratiques.

136. La fonction conformité est indépendante de la direction, afin d'éviter toute influence indue et tout obstacle à l'exercice de ses responsabilités. Elle doit rendre directement compte au conseil d'administration des efforts déployés par la banque dans les domaines susmentionnés et de la gestion, par la banque, du risque de non-conformité.

137. Pour être efficace, la fonction doit être dotée de l'autorité, de la stature, de l'indépendance et des ressources nécessaires, et avoir la liberté d'entrer en relation avec le conseil d'administration. La direction doit respecter l'indépendance de la fonction conformité et de ses missions, et s'abstenir d'intervenir dans leur accomplissement. Comme indiqué précédemment, le chef de la fonction conformité ne doit pas cumuler ce mandat avec un autre poste clé.

[34] Voir Comité de Bâle sur le contrôle bancaire, *Compliance and the compliance function in banks*, avril 2005, www.bis.org/publ/bcbs113.pdf.

Principe 10 – Audit interne

La fonction d'audit interne doit fournir une assurance indépendante au conseil d'administration et aider le conseil d'administration et la direction à promouvoir un processus de gouvernance efficace et la solidité financière de la banque à long terme.

138. Une fonction d'audit efficace et efficiente constitue la troisième ligne de défense du système de contrôles internes. Elle fournit au conseil d'administration et à la direction une garantie indépendante quant à la qualité et à l'efficacité des systèmes et processus de contrôles internes, de gestion des risques et de gouvernance, aidant ainsi le conseil d'administration et la direction à protéger l'organisation et sa réputation[35].

139. La fonction d'audit interne doit avoir un mandat clair, rendre compte au conseil et être indépendante des activités qu'elle vérifie. Elle doit être dotée du statut, des compétences, des ressources et de l'autorité suffisantes au sein de la banque pour que les auditeurs puissent accomplir leur mission avec efficacité et objectivité.

140. Le chef de la fonction audit interne ne doit pas cumuler ce mandat avec un autre poste clé.

141. Le conseil d'administration et la direction contribuent à l'efficacité de la fonction audit interne en :

- accordant à ses membres un accès libre et sans réserve à la totalité des archives, des données et des locaux de la banque, y compris les systèmes et documents d'information de gestion ainsi que les procès-verbaux des réunions de tous les organes consultatifs et de décision ;
- sollicitant une évaluation indépendante de l'efficacité et de l'efficience des systèmes et procédures de contrôles internes, de gestion des risques et de gouvernance ;
- imposant le respect des normes d'audit, tant nationales qu'internationales, comme celles établies par l'Institut des auditeurs internes ;
- exigeant de ses membres qu'ils disposent collectivement des connaissances, compétences et ressources adaptées aux activités et aux risques de la banque ou qu'ils puissent y avoir accès ;
- demandant à la direction de remédier de façon efficace et sans délai aux problèmes en matière d'audit ;
- chargeant la fonction de réaliser une évaluation régulière du dispositif général de gouvernance du risque, et notamment de :
    - l'efficacité des fonctions gestion des risques et conformité ;
    - la qualité des rapports sur les risques soumis au conseil d'administration et à la direction ;
    - l'efficacité du système de contrôles internes de la banque.

142. Le conseil d'administration et la direction doivent respecter et promouvoir l'indépendance de la fonction d'audit interne en mettant en place les conditions suivantes :

- les rapports d'audit interne sont transmis au conseil d'administration, ou à son comité d'audit, sans ingérence de la direction, et les auditeurs internes ont directement accès au conseil d'administration ou à son comité d'audit ;
- le chef de l'audit interne est placé sous la responsabilité directe du conseil d'administration (ou de son comité d'audit), qui est également chargé de le sélectionner, de surveiller sa performance et, le cas échéant, de le révoquer ;
- la révocation du responsable de l'audit interne est rendue publique, et la banque doit justifier cette décision auprès de son autorité de contrôle.

[35] Voir Comité de Bâle sur le contrôle bancaire, *The internal audit function in banks*, 2012, www.bis.org/publ/bcbs223.pdf.

Principe 11 – Rémunération

La structure de rémunération doit contribuer à une saine gouvernance d'entreprise et à la bonne gestion des risques de la banque.

143. Le système de rémunération est un élément central de la gouvernance et du régime d'incitations par lesquels le conseil d'administration et la direction d'une banque encouragent une bonne gouvernance, des comportements acceptables en termes de prise de risque et une solide culture opérationnelle et du risque. Le conseil d'administration (ou, par délégation, son comité des rémunérations) est chargé de surveiller globalement la mise en œuvre, par la direction, du système de rémunération dans l'ensemble de la banque. En outre, le conseil ou son comité doit régulièrement suivre et analyser les résultats du système de rémunération à l'échelle de la banque afin de déterminer s'il crée les incitations permettant une bonne gestion des risques, des fonds propres et de la liquidité[36]. Le conseil d'administration ou son comité doit examiner les plans, procédures et résultats en matière de rémunérations au moins une fois par an.

144. Les établissements financiers d'importance systémique doivent disposer, au sein du conseil d'administration, d'un comité des rémunérations qui fasse partie intégrante de leur structure de gouvernance et surveille l'élaboration et le fonctionnement du système de rémunérations.

145. Les principes du CSF en matière de rémunération sont destinés aux grands établissements financiers, mais ils sont particulièrement importants pour les grandes sociétés d'importance systémique. Les juridictions nationales peuvent également adapter ces principes pour les établissements plus petits et moins complexes. Les banques sont encouragées à mettre en œuvre les principes du CSF ou des dispositions nationales similaires, fondées sur ces principes.

146. Le conseil d'administration, le cas échéant en collaboration avec son comité des rémunérations, doit approuver la rémunération des hauts dirigeants (directeur général, directeur de la gestion des risques et chef de l'audit interne, notamment), et il doit surveiller l'élaboration et le fonctionnement des politiques et systèmes de rémunération ainsi que des processus de contrôle y afférents.

147. La rémunération du personnel des fonctions de contrôle (gestion des risques, conformité et audit interne) doit être déterminée indépendamment des lignes de métier surveillées, et les indicateurs de performance doivent principalement mesurer la réalisation des objectifs de ces fonctions afin de ne pas compromettre leur indépendance.

148. La structure de rémunération doit être en adéquation avec la stratégie en matière d'activité et de risque, les objectifs, les valeurs et les intérêts de la banque à long terme. Elle doit également intégrer des mesures visant à éviter les conflits d'intérêts. Les programmes de rémunération doivent promouvoir une saine culture du risque, incitant les employés à prendre des risques appropriés et à agir dans l'intérêt de la banque dans son ensemble (et notamment de sa clientèle) plutôt que dans leur propre intérêt ou celui de leur unité opérationnelle. En particulier, les incitations intégrées dans les structures de rémunération ne doivent pas encourager les employés à prendre des risques excessifs.

149. La rémunération doit refléter la prise de risque et ses résultats. La pratique consistant à rémunérer des revenus futurs potentiels, dont la réalisation est incertaine, doit faire l'objet d'une évaluation rigoureuse au moyen d'indicateurs tant qualitatifs que quantitatifs. La structure des rémunérations doit permettre d'ajuster la part variable de la rémunération en fonction de l'ensemble des risques, y compris le non-respect de l'appétence pour le risque, des procédures internes ou des obligations légales.

150. Chaque banque doit prévoir des dispositions spécifiques pour les employés ayant une influence significative sur le profil de risque général parce qu'ils sont susceptibles de prendre des risques importants.

[36] En application du document *Implementing the FSB principles for sound compensation practices and their implementation standards – second progress report*, 26 août 2013, p. 14.

Le calendrier de versement des rémunérations doit tenir compte des résultats de la prise de risque sur un horizon de plusieurs années. En ce qui concerne les risques importants, cet horizon est souvent pris en considération grâce à des dispositions visant à différer une part suffisamment importante de la rémunération jusqu'à ce que les résultats de la prise de risque soient mieux connus. Il peut s'agir de mécanismes de malus ou de confiscation, en vertu desquels la rémunération peut être réduite ou annulée sur la base des risques ou comportements réalisés avant que le droit à rémunération soit acquis, mais aussi de mécanismes de restitution, qui prévoient la réduction ou l'annulation éventuelle de la rémunération après versement, si de nouveaux éléments montrent que la rémunération versée se fondait sur des hypothèses erronées, résultant par exemple de rapports falsifiés, ou s'il s'avère que l'employé a enfreint les politiques internes ou des obligations légales. Dans de tels cas, la banque doit prendre, au plus tôt, des mesures pour récupérer les montants versés afin d'accroître la probabilité d'un recouvrement complet. Les primes de bienvenue et les indemnités de départ, qui octroient aux dirigeants ou employés des sommes élevées indépendamment de leurs performances, ne constituent généralement pas de saines pratiques de rémunération.

Principe 12 – Information et transparence

La gouvernance de la banque doit être suffisamment transparente à l'égard des actionnaires, des déposants, des autres parties prenantes et des intervenants de marché.

151. La transparence s'inscrit dans la logique d'une gouvernance d'entreprise saine et efficace. Comme le soulignent les recommandations du Comité de Bâle en matière de transparence bancaire[37], si la transparence est insuffisante, il est difficile pour les actionnaires, les déposants, les autres parties prenantes et les intervenants de marché d'assurer un suivi effectif de l'action du conseil d'administration et de la direction, et de les en tenir dûment responsables. La transparence a donc pour objectif, dans le domaine de la gouvernance d'entreprise, d'apporter à ces parties les informations qui leur permettent d'évaluer l'efficacité de la gouvernance mise en œuvre par le conseil d'administration et la direction de la banque.

152. Même si les banques non cotées en bourse, en particulier celles détenues à 100 %, sont parfois soumises à des obligations de publicité moins détaillées, elles peuvent toutefois poser les mêmes types de risque au système financier que les banques cotées et ce, à divers titres, notamment par leur participation aux systèmes de paiement et leur acceptation de dépôts de détail.

153. Toutes les banques, y compris les banques non cotées qui peuvent être soumises à d'autres normes de publicité, doivent communiquer des informations pertinentes et utiles sur les éléments clés de la gouvernance d'entreprise définis par le Comité de Bâle. Les informations publiées doivent être proportionnelles à la taille, à la complexité, à la structure, au poids économique et au profil de risque de la banque. Au minimum, une banque doit publier les informations suivantes chaque année :

- les critères de sélection des membres du conseil d'administration et la démarche suivie pour assurer la diversité requise en termes de compétences, d'antécédents professionnels et de points de vue ;
- le cas échéant, l'intitulé des comités créés au sein du conseil d'administration et le nombre de réunions des principaux comités permanents.

154. En règle générale, chaque banque doit appliquer la section des principes de l'OCDE consacrée à la transparence et à la diffusion de l'information[38]. Par conséquent, elle doit communiquer les informations importantes qui concernent par exemple : les objectifs de la banque, ses structures et politiques de gouvernance (en particulier le contenu du code ou de la politique de gouvernance ou de rémunération, le cas échéant, et le processus de mise en œuvre), les participations au capital et droits de vote y afférents, et les transactions avec des parties liées. Les banques qui sont tenues de communiquer leurs politiques d'incitations et de rémunération doivent suivre les principes du CSF en matière de rémunération. En particulier, elles doivent publier un rapport annuel sur les questions de rémunération, présentant notamment : le processus décisionnel à l'origine de la politique de rémunération au niveau de la banque, les principales caractéristiques du système de rémunérations (dont les critères utilisés pour mesurer la performance et adapter le niveau de risque), et des informations quantitatives agrégées sur les rémunérations, mais aussi des indicateurs de performance de la banque sur le long terme.

155. Les banques doivent également publier, sans contrevenir à l'obligation de confidentialité, les points clés de leurs stratégies d'exposition au risque et de gestion des risques. Lorsqu'il s'agit d'activités

[37] Comité de Bâle sur le contrôle bancaire, *Renforcement de la transparence bancaire*, septembre 1998, www.bis.org/publ/bcbs41fr.pdf, et *Review of the Pillar 3 disclosure requirements*, juin 2014, www.bis.org/publ/bcbs286.pdf; et CSF, *Enhancing the risk disclosures of banks – report of the Enhanced Disclosure Task Force*, octobre 2012, www.financialstabilityboard.org/publications/r_121029.pdf.

[38] D'après la section V des Principes de l'OCDE : « Un régime de gouvernement d'entreprise doit garantir la diffusion en temps opportun d'informations exactes sur tous les sujets significatifs concernant l'entreprise, notamment la situation financière, les résultats, l'actionnariat et le gouvernement de cette entreprise ». Voir OCDE (2004), op. cit.

importantes, complexes ou peu transparentes, elles doivent communiquer suffisamment d'éléments concernant leurs buts, stratégies, structures, risques et contrôles associés.

156. Les informations publiées doivent être exactes, claires et présentées de façon à ce que les actionnaires, les déposants, les autres parties prenantes et les intervenants de marché puissent y accéder aisément. Il est souhaitable qu'une banque publie des informations à jour sur son site web, dans ses rapports financiers annuels et périodiques et par tout autre moyen pertinent. Il est recommandé de faire figurer une déclaration annuelle détaillée sur la gouvernance d'entreprise dans une section clairement identifiable du rapport annuel, suivant le cadre de communication financière en vigueur. Tout changement important survenu entre deux rapports périodiques doit être communiqué à l'autorité de contrôle de la banque et aux parties prenantes intéressées conformément à la loi et sans retard injustifié.

Principe 13 – Rôle des autorités de contrôle

Il incombe aux autorités de contrôle de formuler des recommandations en matière de gouvernance des banques et d'en contrôler l'application, notamment par le biais d'évaluations exhaustives et de contacts réguliers avec le conseil d'administration et la direction. Elles doivent en outre imposer des améliorations et des mesures correctives, si nécessaire, et partager des informations sur la gouvernance d'entreprise avec les autres autorités de contrôle.

157. Le conseil d'administration et la direction étant les principaux responsables de la gouvernance de la banque, les autorités de contrôle doivent évaluer leurs performances à cet égard. La présente section expose plusieurs principes à même d'aider les autorités de contrôle à évaluer la gouvernance d'entreprise et à favoriser une bonne gouvernance des banques.

Orientations reflétant les attentes en matière de saine gouvernance d'entreprise

158. Les autorités de contrôle doivent définir des orientations ou des règles, conformes aux principes énoncés dans le présent document, qui imposent aux banques de se doter de politiques et de pratiques solides en matière de gouvernance d'entreprise. Ces orientations revêtent une importance particulière lorsque, au niveau national, les lois, règlements, codes ou règles de cotation ne sont pas assez complets pour couvrir les besoins spécifiques des banques en matière de gouvernance d'entreprise. Les orientations réglementaires doivent notamment préciser les attentes concernant l'équilibre des pouvoirs et définir clairement l'attribution des responsabilités, des obligations de rendre compte et des exigences de transparence, entre les membres du conseil d'administration et de la direction, d'une part, et au sein de la banque, d'autre part. Outre l'établissement de ces règles et orientations, les autorités de contrôle doivent, le cas échéant, partager les meilleures pratiques du secteur en matière de gouvernance d'entreprise avec les banques qu'elles supervisent.

Évaluation exhaustive de la gouvernance d'une banque

159. Les autorités de contrôle doivent disposer de procédures leur permettant d'évaluer toutes les composantes de la gouvernance d'une banque. Cette évaluation peut prendre la forme de consultations de documents écrits et de rapports, d'entretiens avec des membres du conseil d'administration et du personnel de la banque, d'examens, d'auto-évaluations de la banque, et d'autres formes de suivi, sur site ou hors site. Elle doit également s'appuyer sur des contacts réguliers avec le conseil d'administration de la banque, la direction, les responsables des fonctions gestion des risques, conformité et audit interne ainsi qu'avec les auditeurs externes[39].

160. Les autorités de contrôle doivent déterminer si la banque est dotée de mécanismes permettant au conseil d'administration et à la direction de s'acquitter de leurs fonctions de surveillance respectives. Elles doivent également vérifier que le conseil d'administration et la direction disposent de procédures pour surveiller les objectifs stratégiques de la banque : appétence pour le risque, performance financière, adéquation et planification des fonds propres, liquidité, profil de risque et culture du risque, contrôles, pratiques de rémunération, et sélection et évaluation des membres de la direction, notamment. Les autorités de contrôle doivent accorder une attention particulière à la surveillance des fonctions gestion des risques, conformité et audit interne. Elles doivent notamment évaluer la portée du dialogue et la fréquence des réunions entre le conseil d'administration et les représentants de ces fonctions. Les autorités

[39] Les auditeurs externes peuvent partager leurs informations avec les autorités de contrôle sans manquer à l'obligation de confidentialité (voir Comité de Bâle, *External audits of banks*, 2014, paragraphes 95 et 96).

de contrôle doivent déterminer si les contrôles internes sont correctement évalués et s'ils contribuent à la saine gouvernance de la banque dans son ensemble.

161. Les autorités de contrôle doivent évaluer les processus et critères de sélection des membres du conseil d'administration et de la direction et, lorsqu'elles l'estiment nécessaire, obtenir des informations sur les compétences professionnelles et les qualités morales des membres du conseil d'administration et de la direction. Les critères de compétence et d'honorabilité utilisés doivent reprendre ceux qui sont mentionnés au Principe 2 du présent document. Le caractère adéquat des qualifications individuelles et collectives des membres du conseil d'administration et de la direction doit faire l'objet d'une attention constante de la part des autorités de contrôle.

162. Lors de leur évaluation générale de la gouvernance d'entreprise d'une banque, les autorités de contrôle doivent également s'attacher à évaluer l'efficacité de la gouvernance du conseil d'administration et de la direction, en particulier s'agissant de la culture du risque. Cette évaluation vise à déterminer dans quelle mesure le comportement du conseil d'administration et de la direction contribue à la bonne gouvernance de la banque. Elle prend en considération la dynamique comportementale du conseil d'administration et de la direction – par exemple, comment l'exemple venu « d'en haut » et les valeurs culturelles de la banque sont transmises et appliquées, comment l'information circule depuis et vers le conseil d'administration et la direction, et comment les problèmes potentiellement graves sont dépistés et traités au sein de l'organisation. Elle repose également sur un examen d'éventuelles évaluations du conseil d'administration et de la direction, d'enquêtes et autres informations souvent utilisées par les banques pour évaluer leur culture interne, ainsi que d'entretiens, d'observations et d'appréciations qualitatives émanant des autorités prudentielles. Lorsqu'elle formule ces appréciations, l'autorité de contrôle doit être particulièrement attentive à respecter l'égalité de traitement entre les banques placées sous sa supervision. Le personnel de l'autorité de contrôle doit être doté des compétences nécessaires pour traiter ces questions et formuler les appréciations complexes que suppose l'évaluation de l'efficacité de la gouvernance.

163. Dans le cas d'une structure de groupe, l'autorité de contrôle doit tenir compte tant des responsabilités de la société mère que de celles de ses filiales en matière de gouvernance, conformément au Principe 5 du présent document.

Contacts réguliers avec le conseil d'administration et la direction

164. L'autorité de contrôle doit avoir des contacts réguliers avec le conseil d'administration et des administrateurs, avec les membres de la direction et avec les responsables des fonctions gestion des risques, conformité et audit interne. Ces contacts doivent prendre notamment la forme de réunions programmées et d'échanges *ad hoc*, par différents moyens de communication (courriel, téléphone, réunions). Ils visent à favoriser l'instauration d'un dialogue ouvert et régulier entre la banque et l'autorité de contrôle sur toute une série de questions : les stratégies de la banque, son modèle opérationnel et les risques auxquels elle est exposée, l'efficacité de sa gouvernance d'entreprise, sa culture, les problèmes de gestion et les plans de succession, les rémunérations et incitations, et d'autres conclusions ou attentes prudentielles que le conseil d'administration doit, d'après l'autorité de contrôle, considérer comme importantes. Par ailleurs, l'autorité de contrôle doit fournir à la banque des indications sur ses activités par rapport aux autres banques, à l'évolution du marché et aux risques systémiques émergents.

165. La fréquence des contacts avec les personnes susmentionnées peut varier selon la taille, la complexité, la structure, le poids économique et le profil de risque de la banque. Ainsi, l'autorité de contrôle peut, par exemple, ne se réunir avec l'ensemble du conseil d'administration qu'une fois par an et s'entretenir plus souvent avec son président, son responsable ou l'administrateur indépendant principal ou encore avec les présidents des principaux comités. Dans le cas des banques d'importance systémique, les contacts doivent être plus fréquents, en particulier avec les membres du conseil et de la direction ainsi qu'avec les responsables des fonctions gestion des risques, conformité et audit interne.

Demandes d'améliorations et d'actions correctives

166. L'autorité de contrôle doit disposer d'un ensemble d'outils lui permettant de répondre aux besoins d'amélioration et aux défaillances en matière de gouvernance. Elle doit être en mesure d'imposer des améliorations et des mesures correctives et d'obliger une banque à rendre compte de sa gouvernance d'entreprise. Elle doit ainsi pouvoir contraindre une banque à changer ses politiques et ses pratiques, à modifier la composition du conseil d'administration et de la direction ou à adopter d'autres actions correctives. De même, elle doit être habilitée, si nécessaire, à infliger des sanctions ou d'autres mesures punitives. Le choix des outils et le délai d'exécution des actions correctives doivent être proportionnés au niveau de risque que l'insuffisance représente pour la sécurité et la solidité de la banque ou du système financier considéré.

167. Lorsqu'une autorité de contrôle demande à une banque de prendre des actions correctives, elle doit également établir un calendrier de mise en œuvre. L'autorité doit disposer d'une procédure d'alerte de la hiérarchie pour exiger des actions correctives plus rigoureuses ou accélérées, au cas où une banque ne remédie pas convenablement aux insuffisances recensées ou si l'autorité estime qu'il y a lieu de prendre des mesures supplémentaires.

Coopération et échange d'informations relatives à la gouvernance d'entreprise avec d'autres autorités compétentes

168. La coopération et les échanges d'informations entre autorités publiques compétentes (notamment celles chargées du contrôle bancaire et de la mise en œuvre des politiques) peuvent accroître l'efficacité de ces instances dans leurs rôles respectifs. Il est particulièrement important que les autorités de contrôle des pays d'origine et d'accueil des banques transfrontières partagent les informations dont elles disposent[40]. La coopération peut être bilatérale et prendre la forme d'un collège prudentiel ou de rencontres régulières lors desquelles les autorités de contrôle abordent les questions de gouvernance d'entreprise[41]. Ce type d'échanges peut, en effet, permettre aux autorités prudentielles de mieux évaluer la gouvernance globale d'une banque et les risques qui pèsent sur elle, en particulier lorsqu'elle appartient à un groupe, et aider d'autres autorités à jauger les risques afférents au système financier dans son ensemble. L'échange doit porter sur des informations pertinentes d'un point de vue prudentiel et respecter les règles de confidentialité et les lois en vigueur. Des dispositions particulières, comme un protocole d'accord, peuvent s'avérer justifiées pour régir les échanges d'informations entre superviseurs ou entre les superviseurs et d'autres autorités.

[40] Voir Comité de Bâle sur le contrôle bancaire, *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012, www.bis.org/publ/bcbs230_fr.pdf, Principe 13 (Relations entre les autorités du pays d'origine et du pays d'accueil).

[41] Voir Comité de Bâle sur le contrôle bancaire, *Principes pour des collèges prudentiels efficaces*, juin 2014, www.bis.org/publ/bcbs287_fr.pdf.