EBA/GL/2017/11

21/03/2018

Orientations

sur la gouvernance interne

1. Obligations de conformité et de déclaration

Statut de ces orientations

1. Le présent document contient des orientations émises en vertu de l'article 16 du règlement (UE) n° 1093/2010 [1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces orientations.

2. Les orientations donnent l'avis de l'ABE sur des pratiques de surveillance appropriées au sein du système européen de surveillance financière ou sur les modalités d'application du droit de l'Union dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) n° 1093/2010, qui sont soumises aux orientations, doivent les respecter en les intégrant dans leurs pratiques, s'il y a lieu (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations s'adressent principalement à des établissements.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles respectent ou entendent respecter ces orientations, ou indiquer les raisons du non-respect des orientations, le cas échéant, avant le 21.05.2018 En l'absence d'une notification avant cette date, les autorités compétentes seront considérées par l'ABE comme n'ayant pas respecté les orientations. Les notifications sont à adresser à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site internet de l'ABE et en indiquant en objet «EBA/GL/2017/11». Les notifications doivent être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes. Toute modification du statut de conformité avec les orientations doit être signalée à l'ABE.

4. Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3.

[1] Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (l'Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331, 15.12.2010, p.12).

2. Objet, champ d'application et définitions

Objet

5. Les présentes orientations précisent les dispositifs, les processus et les mécanismes en matière de gouvernance interne que les établissements de crédit et les entreprises d'investissement doivent mettre en œuvre, conformément à l'article 74, paragraphe 1, de la directive 2013/36/UE[2] afin de garantir une gestion efficace et prudente de l'établissement.

Destinataires

6. Les présentes orientations sont destinées aux autorités compétentes au sens de l'article 4, paragraphe 1, point 40), du règlement (UE) n° 575/2013[3], y compris la Banque centrale européenne en ce qui concerne les questions se rapportant aux tâches qui lui sont confiées par le règlement (UE) n° 1024/2013, et aux établissements au sens de l'article 4, paragraphe 1, point 3), du règlement (UE) n° 575/2013.

Champ d'application

7. Les présentes orientations s'appliquent par rapport auxdispositifs de gouvernance des établissements, y compris leur structure organisationnelle et le partage des responsabilités correspondant, les processus de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, ainsi que le cadre de contrôle interne.

8. Les orientations visent à prendre en compte l'ensemble des structures existantes sans privilégier l'une d'entre elles en particulier. Les orientations n'influent pas sur la répartition globale des compétences conformément au droit national des sociétés. Par conséquent, elles devraient être appliquées indépendamment de la structure utilisée (structure moniste et/ou dualiste et/ou autre structure) dans tous les États membres. L'organe de direction, au sens de l'article 3, paragraphe 1, points 7) et 8), de la directive 2013/36/UE, devrait s'entendre comme ayant des fonctions exécutives et de surveillance (non exécutive)[4].

9. Les termes «organe de direction dans sa fonction exécutive» et «organe de direction dans sa fonction de surveillance» sont utilisés dans l'ensemble de ces orientations sans référence à

[2] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176, 27.6.2013, p. 338).

[3] Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1-337).

[4] Voir également considérant 56 de la directive 2013/36/UE.

quelque structure de gouvernance spécifique que ce soit et les références à la fonction exécutive ou de surveillance (non exécutive) désignent les organes ou les membres de l'organe de direction responsables de cette fonction conformément au droit national. Lorsqu'elles mettent en œuvre les présentes orientations, les autorités compétentes devraient tenir compte de leur droit national des sociétés et préciser, le cas échéant, l'organe ou les membres de l'organe de direction à qui ces orientations devraient s'appliquer.

10. Dans les États membres où l'organe de direction délègue, en tout ou en partie, les fonctions exécutives à une personne ou à un organe exécutif interne (par exemple, un directeur général, une équipe de direction ou un comité exécutif), les personnes exerçant ces fonctions exécutives sur la base de cette délégation devraient être considérées comme constituant la fonction exécutive de l'organe de direction. Aux fins des présentes orientations, toute référence à l'organe de direction dans sa fonction exécutive devrait s'entendre comme incluant également les membres de l'organe exécutif ou le directeur général, au sens des présentes orientations, même s'ils n'ont pas été proposés ou nommés comme membres officiels de l'organe/des organes de direction de l'établissement en vertu du droit national.

11. Dans les États membres où certaines responsabilités sont exercées directement par les actionnaires, les membres ou les propriétaires de l'établissement, au lieu de l'organe de direction, les établissements devraient veiller à ce que ces responsabilités et les décisions y afférentes soient, autant que possible, conformes aux orientations applicables à l'organe de direction.

12. Les définitions de directeur général, de directeur financier et de titulaire de poste clé utilisées dans les présentes orientations sont purement fonctionnelles et ne visent pas à imposer la nomination de ces cadres ou la création de ces postes, à moins que cela ne soit prescrit par le droit pertinent national ou de l'UE.

13. Les établissements devraient respecter, et les autorités compétentes devraient veiller à ce que les établissements respectent, les présentes orientations sur base individuelle, sous-consolidée et consolidée, conformément au niveau d'application prévu à l'article 109 de la directive 2013/36/UE.

Définitions

14. Sauf indication contraire, les termes employés et définis dans la directive 2013/36/UE revêtent la même signification dans les orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

Appétit pour le risque	le niveau et les types agrégés de risque qu'un établissement est prêt à accepter dans le cadre de sa capacité à prendre des risques, conformément à son modèle d'entreprise, afin d'atteindre ses objectifs stratégiques.

Capacité à prendre des risques	le niveau maximal de risque qu'un établissement est en mesure d'accepter compte tenu de son assise financière, de ses capacités de gestion et de contrôle des risques, ainsi que des contraintes réglementaires auxquelles il est soumis.
Culture du risque	les normes, attitudes et comportements d'un établissement en rapport avec la connaissance du risque, la prise de risque et la gestion des risques, ainsi que les contrôles qui déterminent les décisions en matière de risque. La culture du risque influence les décisions de la direction et des employés dans les activités quotidiennes et a une incidence sur les risques dont ils assument la responsabilité.
Établissements	les établissements de crédit et les entreprises d'investissement respectivement au sens de l'article 4, paragraphe 1, points 1) et 2), du règlement (UE) n° 575/2013.
Personnel	l'ensemble des employés d'un établissement et de ses filiales entrant dans son périmètre de consolidation, y compris les filiales ne relevant pas de la directive 2013/36/UE, et l'ensemble des membres de l'organe de direction dans sa fonction exécutive et dans sa fonction de surveillance.
Directeur général	la personne en charge de la gestion et de la direction de l'ensemble des activités d'un établissement.
Directeur financier	la personne globalement en charge de la direction de l'ensemble des activités suivantes: gestion des ressources financières, planification financière et information financière.
Responsables de fonctions de contrôle interne	les personnes au niveau hiérarchique le plus élevé chargées effectivement de diriger le fonctionnement quotidien des fonctions indépendantes de gestion des risques, de vérification de la conformité et d'audit interne.
Titulaires de postes clés	personnes ayant une influence importante sur la direction de l'établissement mais qui ne sont pas membres de l'organe de direction et ne sont pas le directeur général. Ils comprennent les responsables de fonctions de contrôle interne et le directeur financier, lorsqu'ils ne sont pas membres de l'organe de direction, et, lorsqu'ils sont identifiés par les établissements sur la base d'une approche fondée sur les risques, d'autres titulaires de postes clés. Les autres titulaires de postes clés pourraient comprendre les responsables de lignes d'activité importantes, de succursales dans l'Espace économique européen/l'Association européenne de libre-échange, de filiales de pays tiers et d'autres fonctions internes.

Consolidation prudentielle	l'application des règles prudentielles prévues par la directive 2013/36/UE et le règlement (UE) n° 575/2013 sur base consolidée ou sous-consolidée, conformément à la partie 1, titre 2, chapitre 2, du règlement (UE) n° 575/2013. La consolidation prudentielle inclut toutes les filiales qui sont des établissements ou des établissements financiers, respectivement, au sens de l'article 4, paragraphe 1, points 3) et 26), du règlement (UE) n° 575/2013, et peut également inclure des entreprises de services auxiliaires, au sens de l'article 4, paragraphe 1, point 18), dudit règlement, établies dans l'UE ou en dehors de celle-ci.
Établissement consolidant	un établissement tenu de respecter les exigences prudentielles sur base de la situation consolidée, conformément à la partie 1, titre 2, chapitre 2 du règlement (UE) n° 575/2013.
Établissements ayant une importance significative	établissements visés à l'article 131 de la directive 2013/36/UE (établissements d'importance systémique mondiale (EISm) et autres établissements d'importance systémique (autres EIS)) et, le cas échéant, autres établissements déterminés par l'autorité compétente ou la réglementation nationale, sur la base de l'évaluation de la taille et de l'organisation interne des établissements ainsi que de la nature, du champ d'application et de la complexité de leurs activités.
Établissement CRD coté en bourse	établissements dont les instruments financiers sont négociés sur un marché réglementé ou un système multilatéral de négociation, au sens de l'article 4, paragraphe 1, points 21) et 22), de la directive 2014/65/UE, dans un ou plusieurs États membres[5].
Actionnaire	personne propriétaire d'actions d'un établissement ou, selon la forme juridique de l'établissement, autres propriétaires ou membres de l'établissement.
Fonction (de direction)	poste de membre de l'organe de direction d'un établissement ou d'une autre entité juridique.

3. Mise en œuvre

Date d'application

[5] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

15. Les présentes orientations s'appliquent à compter du 30 juin 2018.

Abrogation

16. Les orientations de l'ABE sur la gouvernance interne (GL 44) du 27 septembre 2011 sont abrogées à compter du 30 juin 2018.

4. Orientations

Titre I – Proportionnalité

17. Le principe de proportionnalité codifié à l'article 74, paragraphe 2, de la directive 2013/36/UE vise à garantir que les dispositifs de gouvernance interne sont cohérents avec le profil de risque et le modèle d'entreprise propres à l'établissement, afin que les objectifs des exigences réglementaires soient efficacement atteints.

18. Les établissements devraient tenir compte de leur taille et de leur organisation interne ainsi que de la nature, de l'échelle et de la complexité de leurs activités, lorsqu'ils élaborent et mettent en œuvre des dispositifs de gouvernance interne. Les établissements ayant une importance significative devraient disposer de dispositifs de gouvernance plus sophistiqués, tandis que les établissements de petite taille et moins complexes peuvent mettre en œuvre des dispositifs de gouvernance plus simples.

19. Aux fins de l'application du principe de proportionnalité et afin de garantir une mise en œuvre adéquate des exigences, les établissements et les autorités compétentes devraient tenir compte des critères suivants:

    a. la taille, en termes de bilan, de l'établissement et de ses filiales entrant dans le périmètre de consolidation prudentielle;

    b. la présence géographique de l'établissement et l'ampleur de ses opérations dans chaque juridiction;

    c. La forme juridique de l'établissement, y compris si l'établissement fait partie d'un groupe et, dans l'affirmative, l'évaluation de proportionnalité pour le groupe;

    d. le fait que l'établissement soit coté ou non;

    e. le fait que l'établissement soit autorisé à utiliser des modèles internes pour calculer les exigences de fonds propres (par exemple, l'approche fondée sur les notations internes);

    f. le type d'activités et de services autorisés exercés par l'établissement (par exemple, voir annexe 1 de la directive 2013/36/UE et annexe 1 de la directive 2014/65/UE);

    g. le modèle d'entreprise et la stratégie sous-jacents de l'établissement; la nature et la complexité des activités et la structure organisationnelle de l'établissement ;

h. la stratégie en matière de risque, l'appétit pour le risque et le profil de risque avéré de l'établissement, compte tenu également du résultat des évaluations de l'adéquation du capital et de la liquidité selon le PCEP;

i. la propriété et la structure de financement de l'établissement;

j. le type de clientèle (par exemple, de détail, entreprises, institutionnelle, petites entreprises, entités publiques) et la complexité des produits ou contrats;

k. les activités externalisées et les canaux de distribution; et

l. les systèmes de technologies de l'information existants, y compris les systèmes de continuité et les activités externalisées dans ce domaine.

Titre II – Rôle et composition de l'organe de direction et des comités

1 Rôle et responsabilités de l'organe de direction

20. Conformément à l'article 88, paragraphe 1, de la directive 2013/36/UE, l'organe de direction doit avoir une responsabilité ultime et globale à l'égard de l'établissement et il définit et supervise la mise en œuvre de dispositifs de gouvernance qui garantissent une gestion efficace et prudente de l'établissement et rend des comptes à cet égard.

21. Les attributions de l'organe de direction devraient être clairement définies, établissant une distinction entre la fonction exécutive et la fonction de surveillance (non exécutive). Les responsabilités et les attributions de l'organe de direction devraient être décrites dans un document écrit et dûment approuvées par l'organe de direction.

22. Tous les membres de l'organe de direction devraient être pleinement au fait de la structure et des responsabilités de l'organe de direction et de la séparation des tâches entre les différentes fonctions de l'organe de direction et ses comités. Afin de disposer de contre-pouvoirs appropriés, la prise de décisions au sein de l'organe de direction ne devrait pas être dominée par un seul membre ou un petit sous-ensemble de ses membres. L'interaction entre l'organe de direction dans sa fonction de surveillance et l'organe de direction dans sa fonction exécutive devrait être efficace. Les deux fonctions devraient fournir l'une à l'autre suffisamment d'informations leur permettant d'exercer leurs rôles respectifs.

23. Les responsabilités de l'organe de direction devraient inclure la fixation, l'approbation et la supervision de la mise en œuvre des éléments suivants:

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

b. la stratégie globale en matière de risque, y compris l'appétit pour le risque de l'établissement et son cadre de gestion des risques et les mesures visant à garantir que l'organe de direction consacre suffisamment de temps aux questions relatives aux risques;

c. un cadre adéquat et efficace de gouvernance interne et de contrôle interne comportant une structure organisationnelle claire et des fonctions indépendantes et performantes de gestion des risques, de vérification de la conformité et d'audit disposant d'une autorité, d'un statut et de ressources suffisants pour exercer leurs fonctions;

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

e. les objectifs concernant la gestion de la liquidité de l'établissement;

f. une politique de rémunération conforme aux principes énoncés aux articles 92 à 95 de la directive 2013/36/UE et dans les orientations sur les politiques de rémunération saines au titre des articles 74, paragraphe 3, et 75, paragraphe 2, de la directive 2013/36/UE[6];

g. des dispositifs visant à garantir que les évaluations individuelles et collectives de l'aptitude de l'organe de direction sont réalisées de manière efficace, que la composition et la planification de la succession de l'organe de direction sont appropriées et que l'organe de direction exerce ses fonctions de manière efficace[7];

h. une procédure de sélection et d'évaluation de l'aptitude pour les titulaires de postes clés[8];

i. des dispositifs visant à garantir le fonctionnement interne de chaque comité de l'organe de direction, lorsqu'ils sont instaurés, précisant:

    i. le rôle, la composition et les tâches de chacun d'entre eux;

    ii. le flux d'information approprié, y compris la documentation des recommandations et conclusions, et des systèmes de déclaration entre

[6] Orientations de l'ABE sur les politiques de rémunération saines, au titre des articles 74, paragraphe 3, et 75, paragraphe 2, de la directive 2013/36/UE, et la publication d'informations au titre de l'article 450 du règlement (UE) n° 575/2013 (ABE/GL/2015/22).

[7] Voir également les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

[8] Voir également les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

chaque comité et l'organe de direction, les autorités compétentes et d'autres parties;

j. une culture du risque conforme à la section 9 des présentes orientations, traitant de la connaissance du risque et du comportement en matière de prise de risque de l'établissement;

k. une culture et des valeurs d'entreprise conformes à la section 10, encourageant un comportement responsable et éthique, y compris un code de conduite ou un document similaire;

l. une politique en matière de conflits d'intérêts au niveau de l'établissement conforme à la section 11 et pour le personnel conforme à la section 12; et

m. des dispositifs visant à garantir l'intégrité des systèmes de comptabilité et d'information financière, y compris les contrôles financiers et opérationnels et la vérification de la conformité avec la réglementation et les normes pertinentes.

24. L'organe de direction doit superviser le processus de publication d'informations et de communications avec les parties intéressées externes et les autorités compétentes.

25. Tous les membres de l'organe de direction devraient être informés de l'activité globale, de la situation financière et de la situation en matière de risque de l'établissement, compte tenu de l'environnement économique, ainsi que des décisions adoptées ayant une incidence majeure sur l'activité de l'établissement.

26. Un membre de l'organe de direction peut être responsable d'une fonction de contrôle interne visée au titre V, section 19.1, à condition que ce membre n'ait pas d'autres mandats qui compromettraient ses activités de contrôle interne et l'indépendance de la fonction de contrôle interne.

27. L'organe de direction devrait suivre, examiner périodiquement et pallier les éventuelles faiblesses détectées concernant la mise en œuvre de processus, de stratégies et de politiques se rapportant aux responsabilités énumérées aux points 23 et 24. Le cadre de gouvernance interne et sa mise en œuvre devraient être réexaminés et actualisés périodiquement en tenant compte du principe de proportionnalité, comme expliqué en détail au titre I. Une révision plus approfondie devrait être entreprise lorsque des modifications significatives affectent l'établissement.

2 Fonction exécutive de l'organe de direction

28. L'organe de direction dans sa fonction exécutive devrait participer activement aux activités de l'établissement et devrait adopter des décisions sur une base solide et éclairée.

29. L'organe de direction dans sa fonction exécutive devrait être responsable de la mise en œuvre des stratégies définies par l'organe de direction et discuter régulièrement de la mise en œuvre et de l'adéquation de ces stratégies avec l'organe de direction dans sa fonction de surveillance. La direction de l'établissement peut réaliser la mise en œuvre opérationnelle.

30. L'organe de direction dans sa fonction exécutive devrait remettre en question de manière constructive et examiner d'un œil critique les propositions, les explications et les informations reçues, lorsqu'il exerce son jugement et adopte des décisions. L'organe de direction dans sa fonction exécutive devrait rendre compte sous tous les aspects à l'organe de direction dans sa fonction de surveillance et l'informer régulièrement, et le cas échéant sans délai injustifié, des éléments pertinents pour l'évaluation d'une situation, des risques et des évolutions affectant ou susceptibles d'affecter l'établissement, par exemple des décisions significatives concernant les activités et les risques pris, l'évaluation de l'environnement économique et des affaires dans lequel opère l'établissement, la liquidité et l'assise financière saine ainsi que l'évaluation de ses expositions aux risques d'importance significative.

3 Fonction de surveillance de l'organe de direction

31. Le rôle des membres de l'organe de direction dans sa fonction de surveillance devrait inclure le suivi et la remise en cause de manière constructive de la stratégie de l'établissement.

32. Sans préjudice de la réglementation nationale, l'organe de direction dans sa fonction de surveillance devrait comprendre des membres indépendants, comme prévu à la section 9.3 des orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

33. Sans préjudice des responsabilités attribuées au titre du droit national des sociétés applicable, l'organe de direction dans sa fonction de surveillance devrait:

    a. superviser et suivre la prise de décisions et les actions de la direction et assurer une surveillance efficace de l'organe de direction dans sa fonction exécutive, y compris en suivant et en étudiant ses performances individuelles et collectives et la mise en œuvre de la stratégie et des objectifs de l'établissement;

    b. remettre en question de manière constructive et examiner d'un œil critique les propositions et les informations fournies par les membres de l'organe de direction dans sa fonction exécutive ainsi que ses décisions;

    c. en tenant compte du principe de proportionnalité énoncé au titre I, remplir de manière appropriée les attributions et le rôle du comité des risques, du comité de rémunération et du comité de nomination, lorsque ces comités n'ont pas été instaurés;

d. garantir et évaluer périodiquement l'efficacité du cadre de gouvernance interne de l'établissement et prendre des mesures appropriées afin de remédier aux éventuelles faiblesses détectées;

e. superviser et suivre la mise en œuvre de manière cohérente des objectifs stratégiques, de la structure organisationnelle et de la stratégie en matière de risque de l'établissement, y compris son appétit pour le risque et son cadre de gestion des risques, ainsi que d'autres politiques (par exemple, la politique de rémunération) et le cadre de publication d'informations;

f. contrôler que la culture du risque de l'établissement est mise en œuvre de manière cohérente;

g. superviser la mise en œuvre et le maintien d'un code de conduite ou de politiques similaires et efficaces visant à détecter, gérer et atténuer les conflits d'intérêts avérés et potentiels;

h. superviser l'intégrité des informations financières et des rapports financiers ainsi que le cadre de contrôle interne, y compris un cadre efficace et sain de gestion des risques;

i. garantir que les responsables des fonctions de contrôle interne sont en mesure d'agir de manière autonome et, indépendamment de la responsabilité de rendre des comptes à d'autres organes internes, lignes d'activité ou unités, peuvent exprimer leurs préoccupations et avertir l'organe de direction dans sa fonction de surveillance directement, le cas échéant, lorsque des risques d'évolutions défavorables affectent ou sont susceptibles d'affecter l'établissement; et

j. suivre la mise en œuvre du plan d'audit interne, après la participation préalable des comités des risques et d'audit, lorsque ces comités sont instaurés.

4 Rôle du président de l'organe de direction

34. Le président de l'organe de direction devrait diriger l'organe de direction, devrait contribuer à un flux d'information efficace au sein de l'organe de direction et entre l'organe de direction et ses comités, lorsqu'ils ont été instaurés, et devrait assumer la responsabilité de son fonctionnement efficace global.

35. Le président devrait encourager et favoriser des discussions ouvertes et critiques et s'assurer que les opinions divergentes peuvent être exprimées et débattues dans le cadre du processus de prise de décisions.

36. En principe, le président de l'organe de direction devrait être un membre n'exerçant pas de fonctions exécutives. Si le président peut avoir des attributions exécutives, l'établissement devrait mettre en place des mesures afin d'atténuer toute incidence défavorable sur les contre-pouvoirs de l'établissement (par exemple en désignant un membre éminent ou un

membre indépendant confirmé de l'organe de direction ou en prévoyant un nombre important de membres n'exerçant pas de fonctions exécutives au sein de l'organe de direction dans sa fonction de surveillance). En particulier, conformément à l'article 88, paragraphe 1, point e), de la directive 2013/36/UE, le président de l'organe de direction dans sa fonction de surveillance d'un établissement ne peut pas exercer simultanément la fonction de directeur général dans le même établissement, sauf lorsqu'une telle situation est justifiée par l'établissement et approuvée par les autorités compétentes.

37. Le président devrait établir l'ordre du jour des réunions et assurer que les questions stratégiques sont discutées prioritairement. Il ou elle devrait garantir que les décisions de l'organe de direction sont adoptées de manière judicieuse et éclairée et que les documents et les informations sont reçus dans un délai suffisant avant les réunions.

38. Le président de l'organe de direction devrait contribuer à une répartition claire des attributions entre les membres de l'organe de direction et à l'existence d'un flux d'information efficace entre eux, afin de permettre aux membres de l'organe de direction dans sa fonction de surveillance de contribuer de manière constructive aux discussions et de voter de manière judicieuse et éclairée.

5 Comités de l'organe de direction dans sa fonction de surveillance

5.1 Instaurer des comités

39. Conformément à l'article 109, paragraphe 1, de la directive 2013/36/UE, lu conjointement avec les articles 76, paragraphe 3; 88, paragraphe 2 et 95, paragraphe 1, de la directive 2013/36/UE, tous les établissements ayant une importance significative, compte tenu des niveaux individuel, sous-consolidé et consolidé, doivent instaurer des comités des risques, de nomination[9] et de rémunération[10] qui conseillent l'organe de direction dans sa fonction de surveillance et préparent les décisions à adopter par ledit organe. Les établissements n'ayant pas d'importance significative, y compris lorsqu'ils entrent dans le périmètre de consolidation prudentielle d'un établissement ayant une importance significative dans une situation sous-consolidée ou consolidée, ne sont pas tenus d'instaurer ces comités.

40. Lorsqu'aucun comité des risques ou de nomination n'a été instauré, les références dans les présentes orientations à ces comités devraient être interprétées comme s'appliquant à l'organe de direction dans sa fonction de surveillance, compte tenu du principe de proportionnalité énoncé au titre I.

41. Les établissements peuvent, en tenant compte des critères énoncés au titre I des présentes orientations, instaurer d'autres comités (par exemple, comités de déontologie, de conduite et de vérification de la conformité).

[9] Voir également les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

[10] En ce qui concerne le comité de rémunération, voir les orientations de l'ABE sur les pratiques de rémunération saines.

42. Les établissements devraient garantir une répartition et une distribution claires des attributions et des tâches entre les comités spécialisés de l'organe de direction.

43. Chaque comité devrait recevoir un mandat écrit, précisant la portée de ses responsabilités, de la part de l'organe de direction dans sa fonction de surveillance et établir des procédures de travail appropriées.

44. Les comités devraient apporter leur soutien à la fonction de surveillance dans des domaines spécifiques et faciliter l'élaboration et la mise en œuvre d'un cadre sain de gouvernance interne. La délégation de fonctions aux comités ne décharge en aucun cas l'organe de direction dans sa fonction de surveillance de ses attributions et responsabilités collectives.

5.2 Composition des comités[11]

45. Tous les comités devraient être présidés par un membre de l'organe de direction n'exerçant pas de fonctions exécutives, capable d'exercer un jugement objectif.

46. Les membres indépendants [12] de l'organe de direction dans sa fonction de surveillance devraient participer activement aux comités.

47. Lorsque des comités doivent être instaurés conformément à la directive 2013/36/UE ou à la réglementation nationale, ils devraient être composés d'au moins trois membres.

48. Les établissement devraient s'assurer, en tenant compte de la taille de l'organe de direction et du nombre de membres indépendants de l'organe de direction dans sa fonction de surveillance, que les comités ne sont pas composés du même groupe de membres formant un autre comité.

49. Les établissements devraient envisager la rotation périodique des présidents et membres des comités, en tenant compte de l'expérience, des connaissances et des compétences spécifiques requises à titre individuel ou collectif pour ces comités.

50. Le comité des risques et le comité de nomination devraient être composés de membres n'exerçant pas de fonctions exécutives de l'organe de direction dans sa fonction de surveillance de l'établissement concerné. Le comité d'audit devrait être composé conformément à l'article 41 de la directive 2006/43/CE[13]. Le comité de rémunération devrait

[11] La présente section devrait être lue conjointement avec les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

[12] Au sens de la section 9.3 des orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

[13] Directive 2006/43/CE du Parlement européen et du Conseil du jeudi 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil (JO L 157 du 9.6.2006, p. 87), modifiée en dernier lieu par la directive 2014/56/UE du Parlement européen et du Conseil du 16 avril 2014.

être composé conformément à la section 2.4.1 des orientations de l'ABE sur les politiques de rémunération saines[14].

51. Dans les EISm et les autres EIS, le comité de nomination devrait inclure une majorité de membres indépendants et être présidé par un membre indépendant. Dans les autres établissements ayant une importance significative, déterminés par les autorités compétentes ou par la législation nationale, le comité de nomination devrait inclure un nombre suffisant de membres indépendants; ces établissements peuvent également envisager comme bonne pratique de nommer à la présidence du comité de nomination un membre indépendant.

52. Les membres du comité de nomination devraient disposer, à titre individuel et collectif, de connaissances, de compétences et de l'expertise appropriées concernant le processus de sélection et les exigences d'aptitudes.

53. Dans les EISm et les autres EIS, le comité des risques devrait inclure une majorité de membres indépendants. Dans les EISm et les autres EIS, le président du comité des risques devrait être un membre indépendant. Dans les autres établissements ayant une importance significative, déterminés par les autorités compétentes ou par la législation nationale, le comité des risques devrait inclure un nombre suffisant de membres indépendants et le comité des risques devrait être présidé, autant que possible, par un membre indépendant. Dans tous les établissements, le président du comité des risques ne devrait être ni le président de l'organe de direction ni le président d'un autre comité.

54. Les membres du comité des risques devraient disposer, à titre individuel et collectif, de connaissances, de compétences et de l'expertise appropriées concernant les pratiques de gestion et de contrôle des risques.

5.3 Procédures des comités

55. Les comités devraient faire rapport régulièrement à l'organe de direction dans sa fonction de surveillance.

56. Les comités devraient interagir entre eux, en tant que de besoin. Sans préjudice du point 48, cette interaction pourrait prendre la forme de participation croisée de sorte que le président ou un membre d'un comité puisse également être membre d'un autre comité.

57. Les membres des comités devraient participer à des discussions ouvertes et analytiques, au cours desquelles les différences d'opinion sont discutées de manière constructive.

58. Les comités devraient documenter l'ordre du jour des réunions des comités ainsi que leurs principaux résultats et conclusions.

[14] Orientations de l'ABE sur les politiques de rémunération saines, au titre des articles 74, paragraphe 3, et 75, paragraphe 2, de la directive 2013/36/UE, et la publication d'informations au titre de l'article 450 du règlement (UE) n° 575/2013 (ABE/GL/2015/22).

59. Le comité des risques et le comité de nomination devraient, à tout le moins:

a. avoir accès à toutes les informations et les données pertinentes nécessaires en vue d'exercer leur rôle, y compris des informations et des données de la part des fonctions opérationnelles et de contrôle (par exemple, juridique, finances, ressources humaines, TI, risques, vérification de la conformité, audit etc.);

b. recevoir des rapports réguliers, des informations ad hoc, des communications et des opinions de la part des responsables des fonctions de contrôle interne sur le profil de risque actuel de l'établissement, sa culture du risque et ses limites de risque, ainsi que sur toute violation significative qui a pu avoir lieu, accompagnés d'informations détaillées et de recommandations concernant les mesures correctives adoptées, à adopter ou proposées pour y répondre;

c. décider et réexaminer périodiquement le contenu, le format et la fréquence des informations sur le risque à leur présenter; et

d. s'il y a lieu, garantir la participation adéquate des fonctions de contrôle interne et autres fonctions pertinentes (ressources humaines, juridique, finances) dans leur domaines d'expertise respectifs et/ou solliciter les conseils d'experts externes.

5.4 Rôle du comité des risques

60. Lorsqu'il est instauré, le comité des risques devrait, à tout le moins:

a. fournir ses conseils et son assistance à l'organe de direction dans sa fonction de surveillance en ce qui concerne le suivi de la stratégie globale en matière de risques et d'appétit pour le risque de l'établissement, tant actuels que futurs, en tenant compte de tous les types de risques, afin de garantir qu'ils sont conformes à la stratégie économique, aux objectifs, à la culture et aux valeurs d'entreprise de l'établissement;

b. assister l'organe de direction dans sa fonction de surveillance lorsque celui-ci supervise la mise en œuvre de la stratégie de l'établissement en matière de risque et les limites correspondantes qui ont été fixées;

c. superviser la mise en œuvre des stratégies de l'établissement en matière de gestion des fonds propres et de liquidité ainsi que des autres risques pertinents, tels que le risque de marché, le risque de crédit, le risque opérationnel (y compris les risques juridique et informatique) et le risque de réputation, afin d'évaluer leur adéquation par rapport à l'appétit pour le risque et à la stratégie en matière de risque qui ont été approuvés;

d. fournir à l'organe de direction dans sa fonction de surveillance des recommandations sur les ajustements nécessaires à apporter à la stratégie en matière de risque résultant, entre autres, de modifications du modèle d'entreprise de l'établissement,

d'évolutions du marché ou de recommandations formulées par la fonction de gestion des risques;

e. fournir des conseils concernant le recrutement de consultants externes auxquels la fonction de surveillance peut décider de recourir en vue d'obtenir des avis ou une assistance;

f. examiner différents scénarios possibles, y compris des scénarios de tensions, afin d'évaluer la manière dont le profil de risque de l'établissement réagirait à des événements externes et internes;

g. superviser l'adéquation de tous les produits et services financiers significatifs proposés aux clients avec le modèle d'entreprise et la stratégie en matière de risque de l'établissement [15]. Le comité des risques devrait évaluer les risques associés aux produits et services financiers proposés et tenir compte de la cohérence entre les prix attribués à ces produits et services et les gains générés par ceux-ci; et

h. évaluer les recommandations des auditeurs internes ou externes et suivre la mise en œuvre appropriée des mesures adoptées.

61. Le comité des risques devrait coopérer avec d'autres comités dont les activités peuvent avoir une incidence sur la stratégie en matière de risque (par exemple, le comité d'audit et le comité de rémunération) et communiquer régulièrement avec les fonctions de contrôle interne de l'établissement, notamment avec la fonction de gestion des risques.

62. Lorsqu'il est instauré, le comité des risques doit, sans préjudice des tâches du comité de rémunération, examiner si les incitations inscrites dans les politiques et pratiques de rémunération tiennent compte du risque, du capital et de la liquidité de l'établissement ainsi que de la probabilité et de l'échelonnement dans le temps des bénéfices.

5.5 Rôle du comité d'audit

63. Conformément à la directive 2006/43/CE[16], lorsqu'il est instauré, le comité d'audit devrait, entre autres:

a. suivre l'efficacité des systèmes de contrôle interne de la qualité et de gestion des risques de l'établissement et, le cas échéant, sa fonction d'audit interne, en ce qui

[15] Voir également orientations de l'ABE sur les modalités de gouvernance et de surveillance des produits bancaires de détail, disponibles à l'adresse http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

[16] Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil (JO L 157 du 9.6.2006, p. 87) modifiée en dernier lieu par la directive 2014/56/UE du Parlement européen et du Conseil du 16 avril 2014.

concerne l'information financière de l'établissement contrôlé, sans qu'il soit porté atteinte à son indépendance;

b. superviser la mise en place de politiques comptables par l'établissement;

c. suivre le processus d'élaboration de l'information financière et communiquer des recommandations visant à garantir son intégrité;

d. examiner et contrôler dans la durée l'indépendance des contrôleurs légaux des comptes ou des cabinets d'audit conformément aux articles 22, 22 bis, 22 ter, 24 bis et 24 ter de la directive 2006/43/UE et à l'article 6 du règlement (UE) n° 537/2014[17], et notamment le caractère approprié de la fourniture de services autres que d'audit à l'établissement contrôlé conformément à l'article 5 dudit règlement;

e. vérifier le contrôle légal des états financiers annuels et consolidés, notamment sa réalisation, compte tenu des éventuelles constatations et conclusions de l'autorité compétente en vertu de l'article 26, paragraphe 6, du règlement (UE) n° 537/2014;

f. assumer la responsabilité de la procédure de sélection des contrôleurs légaux des comptes externes ou des cabinets d'audit et soumettre une recommandation, pour approbationpar l'organe compétent de l'établissement (conformément à l'article 16 du règlement (UE) n° 537/2014, sauf lorsque l'article 16, paragraphe 8, du règlement (UE) n° 537/2014 est appliqué), sur leur désignation, rémunération et révocation;

g. réexaminer la portée de l'audit et la fréquence du contrôle légal des états financiers annuels ou consolidés;

h. conformément à l'article 39, paragraphe 6, point a), de la directive 2006/43/UE, communiquer à l'organe d'administration ou de surveillance de l'entité contrôlée des informations sur les résultats du contrôle légal des comptes et des explications sur la façon dont le contrôle légal des comptes a contribué à l'intégrité de l'information financière et sur le rôle que le comité d'audit a joué dans ce processus; et

i. recevoir et tenir compte des rapports d'audit.

5.6 Comités communs

64. Conformément à l'article 76, paragraphe 3, de la directive 2013/36/UE, les autorités compétentes peuvent autoriser des établissements qui ne sont pas considérés comme ayant une importance significative à instaurer un comité commun des risques et d'audit, lorsque ce dernier a été instauré, comme visé à l'article 39 de la directive 2006/43/CE.

[17] Règlement (UE) n° 537/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux exigences spécifiques applicables au contrôle légal des comptes des entités d'intérêt public et abrogeant la décision 2005/909/CE de la Commission (JO L 158 du 27.5.2014, p. 77).

65. Lorsque des comités des risques et de nomination sont instaurés dans des établissements n'ayant pas d'importance significative, ceux-ci peuvent instaurer des comités communs. S'ils le font, ces établissements devraient documenter les raisons pour lesquelles ils ont choisi d'instaurer un comité commun et la manière dont cette approche permet d'atteindre les objectifs des comités.

66. Les établissement devraient garantir à tout moment que les membres d'un comité commun disposent, individuellement et collectivement, des connaissances, des compétences et de l'expertise nécessaires afin de comprendre pleinement les tâches qui devront être accomplies par le comité commun[18].

Titre III – Cadre de gouvernance

6 Cadre organisationnel et structure

6.1 Cadre organisationnel

67. L'organe de direction de l'établissement devrait garantir une structure organisationnelle et opérationnelle appropriée et transparente pour l'établissement et disposer d'une description écrite de cette structure. La structure devrait favoriser et mettre en évidence la gestion efficace et prudente de l'établissement, aux niveaux individuel, sous-consolidé et consolidé. L'organe de direction devrait veiller à ce que les fonctions de contrôle interne soient indépendantes des lignes d'activité qu'elles contrôlent, y compris par une séparation adéquate des attributions, et à ce qu'elles disposent des ressources financières et humaines appropriées ainsi que des pouvoirs pour exercer leur rôle de manière efficace. Les rapports hiérarchiques et la répartition des responsabilités, notamment entre titulaires de postes clés, au sein de l'établissement devraient être clairs, bien définis, cohérents, exécutoires et dûment documentés. La documentation devrait être dûment actualisée.

68. La structure de l'établissement ne devrait pas entraver la capacité de l'organe de direction à superviser et gérer de manière efficace les risques auxquels sont exposés l'établissement ou le groupe ni la capacité de l'autorité compétente à superviser l'établissement de manière efficace.

69. L'organe de direction devrait évaluer si et comment des modifications significatives de la structure du groupe (par exemple, création de nouvelles filiales, fusions et acquisitions, vente ou liquidation de parties du groupe ou évolutions externes) ont une incidence sur la solidité du cadre organisationnel de l'établissement. Lorsque des faiblesses sont détectées, l'organe de direction devrait procéder sans délai à tout ajustement nécessaire.

6.2 Connaissance de sa propre structure

[18] Voir également les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

70. L'organe de direction devrait connaître et comprendre pleinement la structure juridique, organisationnelle et opérationnelle de l'établissement (principe de «connaissance de sa propre structure»), et s'assurer de sa compatibilité avec les stratégies économique, en matière de risque et d'appétit pour le risque qui ont été adoptées.

71. L'organe de direction devrait assumer la responsabilité de l'adoption de stratégies et de politiques saines pour la mise en place de nouvelles structures. Lorsqu'un établissement crée de nombreuses entités juridiques au sein de son groupe, leur nombre, et surtout leurs interconnexions et les transactions exécutées entre elles, ne devraient pas causer de difficultés pour la conception du dispositif de gouvernance interne de l'établissement et pour la gestion et la surveillance efficaces des risques du groupe dans son ensemble. L'organe de direction devrait veiller à ce que la structure de l'établissement et, le cas échéant, les structures au sein du groupe, compte tenu des critères énoncés à la section 7, soient claires, efficaces et transparentes pour le personnel et les actionnaires de l'établissement ainsi que pour les autres parties prenantes et l'autorité compétente.

72. L'organe de direction devrait guider la structure de l'établissement, son évolution et ses limites, et s'assurer qu'elle reste justifiée et efficace et ne présente pas une complexité excessive ou inappropriée.

73. L'organe de direction d'un établissement consolidant devrait comprendre non seulement la structure juridique, organisationnelle et opérationnelle du groupe, mais également la raison d'être et les activités de ses différentes entités, ainsi que leurs liens et relations. Cela inclut la compréhension des risques opérationnels spécifiques au groupe et des expositions intragroupes ainsi que la manière dont les modes de financement, les fonds propres, la liquidité et les profils de risque du groupe pourraient être affectés, tant dans des circonstances normales que dans un contexte défavorable. L'organe de direction devrait garantir que l'établissement est en mesure de produire rapidement des informations sur le groupe, concernant le type, les caractéristiques, l'organigramme, la structure de propriété et les activités de chaque entité et que les établissements au sein du groupe respectent l'ensemble des exigences en matière d'information prudentielle aux niveaux individuel, sous-consolidé et consolidé.

74. L'organe de direction d'un établissement consolidant devrait garantir que les différentes entités du groupe (y compris, l'établissement consolidant lui-même) reçoivent suffisamment d'informations afin d'appréhender clairement les objectifs généraux, les stratégies et le profil de risque du groupe et la manière dont l'entité du groupe concernée est incorporée dans la structure et dans le fonctionnement opérationnel du groupe. Ces informations et leurs révisions devraient être documentées et mises à la disposition des fonctions pertinentes concernées, y compris l'organe de direction, les lignes d'activité et les fonctions de contrôle interne. Les membres de l'organe de direction d'un établissement consolidant devraient se tenir informés des risques causés par la structure du groupe, en tenant compte des critères énoncés à la section 7 des orientations. Cela inclut la réception:

a. d'informations sur les principaux facteurs de risque;

b. de rapports d'évaluation réguliers sur la structure globale de l'établissement et sur la conformité des activités des différentes entités avec la stratégie approuvée pour l'ensemble du groupe;

c. de rapports réguliers sur des questions pour lesquelles le cadre réglementaire exige la conformité aux niveaux individuel, sous-consolidé et consolidé.

6.3 Structures complexes et activités non conventionnelles ou non transparentes

75. Les établissements devraient éviter la mise en place de structures complexes et potentiellement non transparentes. Les établissements devraient tenir compte dans leur prise de décisions des résultats d'une évaluation des risques réalisée afin de détecter si de telles structures pourraient être utilisées dans un but lié au blanchiment de capitaux ou à d'autres délits financiers, ainsi que des contrôles et du cadre juridique respectifs en place[19]. À cet effet, les établissements devraient, à tout le moins, tenir compte des éléments suivants:

a. la mesure dans laquelle la juridiction dans laquelle sera établie la structure respecte effectivement les normes internationales et de l'UE sur la transparence fiscale, la lutte contre le blanchiment de capitaux et le financement du terrorisme;

b. la mesure dans laquelle la structure sert un objectif économique évident et légal;

c. la mesure dans laquelle la structure pourrait être utilisée pour dissimuler l'identité du bénéficiaire effectif final;

d. la mesure dans laquelle la demande du client qui mène à la création possible d'une structure donne lieu à des préoccupations;

e. le fait que la structure puisse entraver la supervision appropriée de la part de l'organe de direction de l'établissement ou la capacité de l'établissement à gérer le risque y afférent; et

f. le fait que la structure comporte des éléments faisant obstacle à une supervision efficace de la part des autorités compétentes.

76. En tout état de cause, les établissements ne devraient pas créer des structures opaques ou inutilement complexes n'ayant pas de raison d'être économique claire ou d'objectif juridique

[19] Pour plus de détails sur l'évaluation du risque de pays et du risque associé à des produits et clients particuliers, les établissements devraient se référer également aux orientations communes finales (une fois publiées) sur les facteurs de risque: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

ou si les établissements craignent que ces structures puissent être utilisées à des fins liées à des délits financiers.

77. Lorsqu'il crée de telles structures, l'organe de direction devrait les comprendre, ainsi que l' objectif et les risques particuliers qui y sont associés et veiller à ce que les fonctions de contrôle interne soient dûment impliquées dans leur mise en place. De telles structures ne devraient être approuvées et maintenues que lorsque leur objectif a été clairement défini et compris et lorsque l'organe de direction a l'assurance que tous les risques significatifs, y compris les risques de réputation, ont été recensés, que tous les risques peuvent être gérés de manière efficace et dûment déclarés et qu'une surveillance efficace a été assurée. Plus la structure organisationnelle et opérationnelle est complexe et opaque et plus les risques sont importants, plus la surveillance de la structure devrait être intensive.

78. Les établissements devraient documenter leurs décisions et être en mesure de les justifier auprès des autorités compétentes.

79. L'organe de direction devrait s'assurer que des mesures appropriées sont prises pour prévenir ou atténuer les risques des activités au sein des ces structures. Cela inclut de veiller à ce que:

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

    b. les informations concernant ces activités et les risques associés à celles-ci soient accessibles à l'établissement consolidant et aux contrôleurs internes et externes et déclarées à l'organe de direction dans sa fonction de surveillance et à l'autorité compétente qui a octroyé l'agrément;

    c. l'établissement évalue périodiquement s'il y a lieu de maintenir de telles structures.

80. Ces structures et activités, y compris leur conformité avec la réglementation et les normes professionnelles, devraient faire l'objet de réexamens réguliers de la part de la fonction d'audit interne selon une approche fondée sur les risques.

81. Les établissements devraient adopter les mêmes mesures de gestion des risques que pour leurs propres activités économiques lorsqu'ils exercent des activités non conventionnelles ou non transparentes pour des clients (par exemple, aider des clients à créer des instruments dans des juridictions extraterritoriales, élaborer des structures complexes, financer pour eux des transactions ou fournir des services fiduciaires), lesquelles créent des difficultés similaires de gouvernance interne ainsi que des risques opérationnels et de réputation significatifs. Les établissements devraient notamment étudier la raison pour laquelle un client souhaite mettre en place une structure particulière.

7 Cadre organisationnel dans le contexte d'un groupe

82. Conformément à l'article 109, paragraphe 2, de la directive 2013/36/UE, les entreprises mères et les filiales relevant de cette directive devraient assurer la cohérence et la bonne intégration des dispositifs, processus et mécanismes de gouvernance sur base consolidée ou sous-consolidée. À cette fin, les entreprises mères et les filiales entrant dans le périmètre de consolidation prudentielle devraient mettre en œuvre de tels dispositifs, processus et mécanismes dans leurs filiales ne relevant pas de la directive 2013/36/UE afin d'assurer un dispositif solide de gouvernance sur base consolidée et sous-consolidée. Les fonctions compétentes au sein de l'établissement consolidant et de ses filiales devraient interagir et échanger des données et des informations, en tant que de besoin. Les dispositifs, processus et mécanismes de gouvernance devraient garantir que l'établissement consolidant dispose de données et d'informations suffisantes et qu'il est en mesure d'évaluer le profil de risque pour l'ensemble du groupe, comme décrit en détail à la section 6.2.

83. L'organe de direction d'une filiale relevant de la directive 2013/36/UE devrait adopter et mettre en œuvre au niveau individuel les politiques de gouvernance établies pour l'ensemble du groupe, au niveau consolidé ou sous-consolidé, de manière à se conformer à l'ensemble des exigences particulières de la législation nationale et de l'UE.

84. Aux niveaux consolidé et sous-consolidé, l'établissement consolidant devrait garantir l'observation des politiques de gouvernance de l'ensemble du groupe par tous les établissements et autres entités entrant dans le périmètre de consolidation prudentielle, y compris leurs filiales ne relevant pas de la directive 2013/36/UE. Lorsqu'il met en œuvre des politiques de gouvernance, l'établissement consolidant devrait garantir la mise en place de dispositifs de gouvernance solides pour chaque filiale et envisager des dispositifs, des processus et des mécanismes spécifiques lorsque les activités économiques ne sont pas organisées dans des entités juridiques séparées mais au sein d'une matrice de lignes d'activité qui inclut plusieurs entités juridiques.

85. L'établissement consolidant devrait tenir compte des intérêts de toutes ses filiales et de la manière dont les stratégies et les politiques contribuent aux intérêts de chaque filiale et aux intérêts du groupe dans son ensemble sur le long terme.

86. Les entreprises mères et leurs filiales devraient veiller à ce que les établissements et les entités au sein du groupe respectent les exigences particulières de toute juridiction pertinente.

87. L'établissement consolidant devrait garantir que les filiales établies dans des pays tiers, entrant dans le périmètre de consolidation prudentielle, ont mis en place des dispositifs, des processus et des mécanismes de gouvernance cohérents avec les politiques en matière de gouvernance de l'ensemble du groupe et respectent les exigences énoncées aux articles 74 à 96 de la directive 2013/36/UE et dans les présentes orientations, à condition que cela ne soit pas illicite au regard de la législation du pays tiers.

88. Les exigences en matière de gouvernance énoncées dans la directive 2013/36/UE et dans les présentes orientations s'appliquent aux établissements indépendamment du fait qu'ils soient ou non les filiales d'une entreprise mère dans un pays tiers. Lorsqu'une filiale établie dans l'Union européenne d'une entreprise mère implantée dans un pays tiers est un établissement consolidant, le périmètre de consolidation prudentielle n'inclut pas le niveau de l'entreprise mère située dans un pays tiers ni d'aucune autre filiale directe de cette entreprise mère. L'établissement consolidant devrait veiller à ce que la politique de gouvernance déployée à l'échelle du groupe de l'établissement mère implanté dans un pays tiers soit prise en compte dans sa propre politique de gouvernance dans la mesure où cela n'est pas contraire aux exigences énoncées dans la réglementation de l'UE, y compris la directive 2013/36/UE et les présentes orientations.

89. Lorsqu'ils mettent en place des politiques et documentent les dispositifs de gouvernance, les établissements devraient tenir compte des aspects énumérés à l'annexe I des orientations. Bien que les politiques et la documentation puissent figurer dans des documents séparés, les établissements devraient envisager de les combiner ou de faire référence à ceux-ci dans un document unique sur le cadre de gouvernance.

8 Politique d'externalisation[20]

90. L'organe de direction devrait approuver et réexaminer et actualiser régulièrement la politique d'externalisation d'un établissement, en veillant à ce que les modifications appropriées soient rapidement mises en œuvre.

91. La politique d'externalisation devrait tenir compte de l'incidence de cette pratique sur les activités de l'établissement et sur les risques auxquels il est exposé (notamment les risques opérationnels, y compris les risques juridique et informatique; les risques de réputation et les risques de concentration). Cette politique devrait inclure les dispositifs de notification et de contrôle qui doivent être mis en œuvre depuis l'entrée en vigueur d'un accord d'externalisation jusqu'à son terme (y compris l'élaboration du dossier d'externalisation, la signature du contrat, l'exécution de ce dernier jusqu'à son expiration, les plans d'urgence et les stratégies de sortie). L'établissement demeure pleinement responsable de l'ensemble des services et activités qu'il externalise, ainsi que des décisions de gestion qui en résultent. Par conséquent, la politique d'externalisation devrait expressément indiquer que cette pratique ne soustrait pas l'établissement à ses obligations réglementaires et à ses responsabilités envers ses clients.

92. La politique devrait préciser que les dispositifs d'externalisation ne peuvent pas entraver les contrôles sur place ou sur pièces de l'établissement et ne peuvent en aucune manière contrevenir aux restrictions émises par le superviseur sur les services et les activités exercés. La politique devrait également couvrir l'externalisation intragroupe (à savoir les services

[20] Les présentes orientations ne portent que sur la politique générale d'externalisation, les questions particulières liées à l'externalisation étant traitées dans les orientations du CECB relatives à l'externalisation, qui seront révisées. Ces orientations sont disponibles à l'adresse https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing (fournir le lien vers la version française).

fournis par une entité juridique séparée au sein du groupe d'un établissement) et tenir compte de toutes circonstances particulières du groupe.

93. La politique devrait prévoir que, lors de la sélection des prestataires externes de services d'importance significative ou d'externalisation des activités, l'établissement doit tenir compte du fait que le prestataire de services dispose ou non de normes déontologiques appropriées ou d'un code de conduite.

Titre IV – Culture du risque et exercice des activités

9 Culture du risque

94. Une culture du risque solide et cohérente devrait être un élément clé de la gestion efficace des risques des établissements et devrait permettre aux établissements d'adopter des décisions judicieuses et éclairées.

95. Les établissements devraient mettre en place une culture du risque intégrée et globale, sur la base d'une entière compréhension et d'une vision holistique des risques auxquels il sont exposés et de la manière dont ils sont gérés, en tenant compte de leur appétit pour le risque.

96. Les établissements devraient élaborer une culture du risque au moyen de politiques, de la communication et de la formation du personnel en ce qui concerne les activités, la stratégie et le profil du risque de l'établissement et ils devraient adapter la communication et la formation du personnel afin de tenir compte des responsabilités du personnel concernant la prise de risque et la gestion des risques.

97. Le personnel devrait être pleinement conscient de ses responsabilités concernant la gestion des risques. La gestion des risques ne devrait pas être la prérogative exclusive des spécialistes du risque ou des fonctions de contrôle interne. Les différentes unités opérationnelles, sous la supervision de l'organe de direction, devraient essentiellement assumer la responsabilité de la gestion quotidienne des risques conformément aux politiques, aux procédures et aux contrôles de l'établissement et en tenant compte de l'appétit pour le risque et de la capacité de l'établissement à prendre des risques.

98. Sans y être nécessairement limitée, une culture du risque solide devrait inclure ce qui suit:

    a. L'exemple de la direction: l'organe de direction devrait être responsable de la définition et de la communication des principales valeurs et attentes de l'établissement. Le comportement de ses membres devrait refléter les valeurs auxquelles l'établissement adhère. La direction des établissements, y compris les titulaires de postes clés, devrait contribuer à la communication interne au personnel des principales valeurs et attentes. Le personnel devrait agir en conformité avec toutes les lois et réglementations applicables et communiquer rapidement au sein ou à l'extérieur de l'établissement (par exemple, à l'autorité compétente par une procédure de dénonciation des dysfonctionnements) les cas de non-conformité

observés. L'organe de direction devrait promouvoir, suivre et évaluer continuellement la culture du risque de l'établissement; examiner l'incidence de la culture du risque sur la stabilité financière, le profil du risque et la gouvernance solide de l'établissement; et procéder à des modifications, lorsqu'il y a lieu.

b. Obligation de rendre compte: les membres du personnel concernéq à tous les niveaux devraient connaître et comprendre les valeurs fondamentales de l'établissement ainsi que, dans la mesure où cela est nécessaire pour exercer leur rôle, son appétit pour le risque et sa capacité à prendre des risques. Ils devraient être en mesure d'exercer leur rôle et être conscient qu'ils devront assumer la responsabilité de leurs actes en rapport avec le comportement de prise de risque de l'établissement.

c. Communication efficace et remise en cause: une culture du risque solide devrait promouvoir un environnement de communication ouverte et de remise en cause efficace dans lequel les processus de prise de décisions encouragent un large échange d'avis, permettent de mettre à l'épreuve les pratiques actuelles, stimulent une attitude constructive et critique au sein du personnel et promeuvent un climat de participation ouverte et constructive dans l'ensemble de l'organisation.

d. Incitations: des incitations appropriées devraient jouer un rôle important dans l'alignement du comportement de prise de risque avec le profil de risque de l'établissement et ses intérêts à long terme[21].

10 Valeurs de l'entreprise et code de conduite

99. L'organe de direction devrait élaborer, adopter, observer et promouvoir des normes déontologiques et professionnelles de haut niveau, en tenant compte des besoins et des caractéristiques propres à l'établissement et devrait garantir la mise en œuvre de ces normes (au moyen d'un code de conduite ou d'un document similaire). Il devrait également superviser le respect de ces normes par le personnel. Le cas échéant, l'organe de direction peut adopter et mettre en œuvre les normes de l'établissement à l'échelle du groupe ou des normes communes émises par des associations ou d'autres organisations pertinentes.

100. Les normes mises en œuvre devraient viser à réduire les risques auxquels l'établissement est exposé, notamment les risques opérationnels et de réputation, qui peuvent avoir une incidence défavorable considérable sur la rentabilité et la durabilité de l'établissement par des amendes, des frais judiciaires, des restrictions imposées par les autorités compétentes, d'autres sanctions financières et pénales ainsi que la perte de valeur de la marque et de la confiance des consommateurs.

101. L'organe de direction devrait mettre en place des politiques claires et documentées concernant la manière dont ces normes devraient être respectées. Ces politiques devraient:

[21] Voir également les orientations de l'ABE sur les politiques de rémunération saines, au titre des articles 74, paragraphe 3, et 75, paragraphe 2, de la directive 2013/36/UE, et la publication d'informations au titre de l'article 450 du règlement (UE) n° 575/2013 (ABE/GL/2015/22), disponibles à l'adresse https://www.eba.europa.eu/regulation-and-policy/remuneration (fournir le lien vers la version française).

a. rappeler aux lecteurs que toutes les activités de l'établissement devraient être menées conformément à la législation applicable et aux valeurs d'entreprise de l'établissement;

b. promouvoir la connaissance du risque par une culture du risque solide conformément à la section 9 des orientations, en communiquant l'attente de l'organe de gestion, à savoir que les activités ne dépasseront pas l'appétit pour le risque et les limites définies par l'établissement ainsi que les responsabilités correspondantes du personnel;

c. énoncer des principes et fournir des exemples de comportements acceptables et inacceptables liés notamment aux fausses déclarations et aux mauvaises conduites financières, à la criminalité économique et financière (y compris la fraude, le blanchiment de capitaux et les pratiques anti-trust, les sanctions financières, la corruption active et passive, la manipulation de marché, la vente abusive et autres violations de la réglementation en matière de protection des consommateurs);

d. préciser que, outre le respect des exigences juridiques et réglementaires et des politiques internes, le personnel est tenu de se comporter avec honnêteté et intégrité et d'exercer ses attributions en faisant preuve de la compétence, du soin et de la diligence requis; et

e. veiller à ce que le personnel soit conscient des éventuelles mesures disciplinaires internes et externes, actions en justice et sanctions que les mauvaises conduites et les comportements inacceptables peuvent entraîner.

102. Les établissements devraient vérifier le respect de ces normes et veiller à la sensibilisation du personnel, par exemple en offrant une formation. Les établissements devraient définir la fonction responsable du contrôle du code de conduite, ou de documents similaires, et de l'évaluation des violations de celui-ci ainsi qu'une procédure pour intervenir en cas de non-respect. Les résultats devraient être communiqués périodiquement à l'organe de direction.

11 Politique en matière de conflits d'intérêts au niveau de l'établissement

103. L'organe de direction devrait être responsable de la mise en place, de l'approbation et de la supervision de la mise en œuvre et du maintien de politiques efficaces destinées à recenser, évaluer, gérer et atténuer ou éviter les conflits d'intérêts avérés et potentiels au niveau de l'établissement, par exemple en raison des différentes activités et des différents rôles de l'établissement, des différents établissements entrant dans le périmètre de consolidation prudentielle, de différentes lignes d'activité ou unités au sein d'un établissement, ou en rapport avec les personnes intéressées externes.

104. Les établissements devraient adopter, dans leurs dispositifs organisationnels et administratifs, des mesures adéquates afin d'éviter que les conflits d'intérêts aient une incidence défavorable sur les intérêts de leurs clients.

105. Les mesures adoptées par les établissements en vue de gérer ou, le cas échéant, atténuer les conflits d'intérêts devraient être documentées et inclure, entre autres, ce qui suit:

    a. une séparation appropriée des attributions, en confiant par exemple à des personnes différentes les activités conflictuelles relevant du traitement des transactions ou de la prestation de services, ou en confiant à des personnes différentes les responsabilités en matière de surveillance et de déclaration pour les activités conflictuelles;

    b. la mise en place de cloisonnements de l'information, par exemple par la séparation physique de certaines lignes d'activité ou unités; et

    c. la mise en place de procédures adéquates concernant les transactions entre parties liées, par exemple en exigeant que les transactions soient réalisées dans des conditions de pleine concurrence.

12 Politique en matière de conflits d'intérêts pour le personnel[22]

106. L'organe de direction devrait être responsable de la mise en place, de l'approbation et de la surveillance de la mise en œuvre et du maintien de politiques efficaces visant à recenser, évaluer, gérer et atténuer ou éviter les conflits avérés et potentiels entre les intérêts de l'établissement et les intérêts privés du personnel, y compris les membres de l'organe de direction, qui pourraient avoir une incidence défavorable sur l'exercice de leurs attributions et responsabilités. Un établissement consolidant devrait envisager les intérêts dans le cadre d'une politique en matière de conflits d'intérêts à l'échelle du groupe sur base consolidée ou sous-consolidée.

107. La politique devrait viser à recenser les conflits d'intérêts du personnel, y compris les intérêts des membres de leur famille les plus proches. Les établissements devraient tenir compte du fait que des conflits d'intérêts peuvent naître non seulement de relations personnelles ou professionnelles actuelles mais également de relations personnelles ou professionnelles antérieures. Lorsqu'un conflit d'intérêts survient, les établissements devraient évaluer son importance et adopter et mettre en œuvre des mesures d'atténuation appropriées.

108. En ce qui concerne les conflits d'intérêts susceptibles de résulter de relations antérieures, les établissements devraient fixer une période appropriée pour laquelle ils souhaitent que le personnel déclare de tels conflits d'intérêts, au motif que ceux-ci peuvent encore avoir une incidence sur le comportement du personnel et influencer la prise de décisions.

109. La politique devrait couvrir à tout le moins les situations ou relations suivantes dans lesquelles des conflits d'intérêts peuvent survenir:

[22] La présente section devrait être lue conjointement avec les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

a. intérêts économiques (par exemple, actions, autres droits de propriété et participations, participations financières et autres intérêts économiques dans des clients commerciaux, droits de propriété intellectuelle, prêts octroyés par l'établissement à une société appartenant à un membre du personnel, participation dans un organe ou propriété d'un organe ou d'une entité ayant des intérêts conflictuels);

b. relations personnelles ou professionnelles avec les détenteurs de participations qualifiées dans l'établissement;

c. relations personnelles ou professionnelles avec un membre du personnel de l'établissement ou d'entités incluses dans le périmètre de consolidation prudentielle (par exemple, relations familiales);

d. autre emploi et emploi antérieur dans le passé récent (par exemple, cinq ans);

e. relations personnelles ou professionnelles avec des parties intéressées externes (par exemple, association avec des fournisseurs ou consultants ou autres prestataires de services d'importance significative); et

f. influence politique ou relations politiques.

110. Nonobstant ce qui précède, les établissements devraient tenir compte du fait que la qualité d'actionnaire d'un établissement ou de titulaire de comptes privés ou d'emprunteur ou d'utilisateur d'autres services d'un établissement ne devrait pas mener à une situation où le membre du personnel est considéré comme ayant un conflit d'intérêts, dès lors qu'il demeure en-deçà d'un seuil de minimis approprié.

111. La politique devrait énoncer les procédures de déclaration et de communication à la fonction responsable au titre de la politique. Le membre du personnel devrait être tenu de déclarer sans délai à l'établissement toute situation susceptible de créer un conflit d'intérêts ou ayant déjà causé un conflit d'intérêts.

112. La politique devrait opérer une distinction entre des conflits d'intérêts qui persistent et qui doivent être gérés de manière permanente et des conflits d'intérêts qui surviennent de manière inattendue en relation avec un événement unique (par exemple une transaction, la sélection d'un prestataire de services etc.) et peuvent généralement être maîtrisés au moyen d'une mesure unique. Dans tous les cas, l'intérêt de l'établissement devrait être l'élément déterminant pour la prise des décisions.

113. La politique devrait énoncer les procédures, les mesures, les exigences en matière de documentation et les responsabilités concernant la détection et la prévention de conflits d'intérêts en vue d'évaluer leur importance et d'adopter des mesures d'atténuation. Ces procédures, exigences, responsabilités et mesures devraient inclure ce qui suit:

a. confier des activités ou des transactions conflictuelles à des personnes différentes;

b. empêcher que des membres du personnel exerçant également une activité en-dehors de l'établissement aient une influence inappropriée au sein de l'établissement en rapport avec ces autres activités;

c. imposer aux membres de l'organe de direction la responsabilité de s'abstenir lors d'un vote sur tout sujet engendrant ou susceptible d'engendrer un conflit d'intérêts ou pour lequel leur objectivité ou leur capacité de remplir correctement leurs obligations envers l'établissement pourraient être compromises de quelqu'autre manière que ce soit;

d. établir des procédures adéquates pour les transactions avec des parties liées (les établissements peuvent envisager, entre autres, d'exiger que les transactions soient réalisées dans des conditions de pleine concurrence, que toutes les procédures de contrôle interne pertinentes s'appliquent pleinement à ces transactions, que des membres indépendants de l'organe de direction émettent leurs avis consultatifs contraignants, que les actionnaires approuvent les transactions les plus pertinentes et que l'exposition à de telles transactions soit limitée); et

e. empêcher les membres de l'organe de direction de détenir des fonctions de direction dans des établissements concurrents, à moins qu'il s'agisse d'établissements faisant partie du même système de protection institutionnel, visé à l'article 113, paragraphe 7, du règlement (UE) n° 575/2013, d'établissements de crédit affiliés de manière permanente à un organisme central, visés à l'article 10 du règlement (UE) n° 575/2013, ou d'établissements entrant dans le périmètre de consolidation prudentielle.

114. La politique devrait couvrir spécifiquement le risque de conflits d'intérêts au niveau de l'organe de direction et fournir suffisamment d'orientations concernant la détection et la gestion de conflits d'intérêts susceptibles d'entraver la capacité des membres de l'organe de direction à adopter des décisions objectives et impartiales visant à répondre au mieux aux intérêts de l'établissement. Les établissements devraient tenir compte du fait que les conflits d'intérêts peuvent avoir une incidence sur l'indépendance d'esprit des membres de l'organe de direction[23].

115. Les conflits d'intérêts avérés ou potentiels qui ont été déclarés à la fonction responsable au sein de l'établissement devraient être dûment évalués et gérés. Si un conflit d'intérêts concernant un membre du personnel est détecté, l'établissement devrait documenter la décision adoptée, notamment si le conflit d'intérêts et les risques associés ont été acceptés, et, si le conflit d'intérêts a été accepté, la manière dont il a été atténué ou dont il y a été remédié de manière satisfaisante.

[23] Voir également les orientations communes de l'AEMF et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés au titre de la directive 2013/36/UE et de la directive 2014/65/UE.

116. Tous les conflits d'intérêts avérés ou potentiels au niveau de l'organe de direction devraient être, individuellement et collectivement, dûment documentés, communiqués à l'organe de direction et discutés, donner lieu à une décision et être dûment gérés par l'organe de direction.

13 Procédures d'alerte interne

117. Les établissements devraient mettre en place et maintenir des politiques et des procédures appropriées en matière d'alerte interne pour que le personnel puisse signaler des violations potentielles ou avérées des exigences réglementaires ou internes, y compris, sans limitation, celles prévues par le règlement (UE) n° 575/2013 et les dispositions transposant la directive 2013/36/UE en droit national, ou des dispositifs de gouvernance internes, par une voie spécifique, indépendante et autonome. Il ne devrait pas être nécessaire que le membre du personnel signalant une violation en possède la preuve; il devrait cependant avoir un niveau de certitude suffisant constituant une raison suffisante pour ouvrir une enquête.

118. Afin d'éviter les conflits d'intérêts, il devrait être possible pour le personnel de signaler des violations en dehors des voies hiérarchiques traditionnelles (par exemple, par l'intermédiaire de la fonction de vérification de la conformité, la fonction d'audit interne ou par une procédure indépendante interne de dénonciation des dysfonctionnements). Les procédures d'alerte devraient garantir la protection des données à caractère personnel tant de la personne qui signale la violation que de la personne physique qui est prétendument responsable de la violation, conformément à la directive 95/46/CE.

119. Les procédures d'alerte devraient être mises à la disposition de l'ensemble du personnel de l'établissement.

120. Les informations fournies par un membre du personnel dans le cadre des procédures d'alerte devraient, le cas échéant, être mises à la disposition de l'organe de direction et des autres fonctions responsables définies dans le cadre de la politique en matière d'alerte interne. Si le membre du personnel signalant une violation le demande, les informations devraient être fournies à l'organe de direction et aux autres fonctions responsables sous une forme anonymisée. Les établissements peuvent également prévoir une procédure de dénonciation des dysfonctionnements permettant la présentation des informations sous une forme anonymisée.

121. Les établissements devraient garantir que la personne signalant la violation est dûment protégée contre toute incidence défavorable, par exemple des représailles, des discriminations ou d'autres types de traitement injuste. L'établissement devrait garantir qu'aucune personne sous le contrôle de l'établissement ne prenne des mesures inéquitables envers une personne ayant signalé une violation et il devrait adopter des mesures appropriées contre les responsables de tels actes.

122. Les établissements devraient également protéger les personnes dénoncées contre toute conséquence défavorable, si l'enquête ne fait apparaître aucune preuve justifiant l'adoption

de mesures contre ces personnes. S'il adopte des mesures, l'établissement devrait le faire de manière à protéger la personne concernée contre les effets défavorables involontaires allant au-delà de l'objectif de la mesure adoptée.

123. Plus précisément, les procédures d'alerte interne devraient:

a. être documentées (par exemple, manuels pour le personnel);

b. prévoir des règles claires garantissant que les informations sur la déclaration et les personnes dénoncées ainsi que sur la violation sont traitées de manière confidentielle, conformément à la directive 95/46/CE, sauf si la divulgation est requise par le droit national dans le cadre d'autres enquêtes ou d'une procédure judiciaire ultérieure;

c. protéger le personnel exprimant ses préoccupations contre des représailles pour avoir divulgué des violations à signaler;

d. garantir que les violations potentielles ou avérées signalées sont évaluées et communiquées, y compris, lorsque cela est approprié, à l'autorité compétente ou aux organismes d'application de la loi;

e. garantir, autant que possible, que le membre du personnel qui signale des violations potentielles ou avérées reçoit une confirmation de la réception des informations;

f. garantir le suivi du résultat d'une enquête concernant une violation signalée; et

g. garantir la conservation appropriée des dossiers.

14 Signaler des violations aux autorités compétentes

124. Les autorités compétentes devraient mettre en place des mécanismes efficaces et fiables permettant au personnel des établissements de signaler aux autorités compétentes des violations pertinentes potentielles ou avérées d'exigences réglementaires, y compris, sans limitation, celles prévues par le règlement (UE) n° 575/2013 et les dispositions transposant la directive 2013/36/UE en droit national. Ces mécanismes devraient inclure à tout le moins:

a. des procédures spécifiques pour la réception de déclarations concernant des violations et pour le suivi de ces déclarations, par exemple un service, une unité ou une fonction dédiée à la dénonciation des dysfonctionnements;

b. une protection appropriée comme prévu à la section 13;

c. la protection des données à caractère personnel tant de la personne physique qui signale la violation que de la personne physique qui est prétendument responsable de la violation, conformément à la directive 95/46/CE; et

d. des procédures claires comme prévu au point 123.

125. Sans préjudice de la possibilité de signaler des violations au moyen des mécanismes des autorités compétentes, celles-ci peuvent encourager le personnel à utiliser en première instance les procédures d'alerte interne de leurs établissements.

Titre V – Cadre et mécanismes de contrôle interne

15 Cadre de contrôle interne

126. Les établissements devraient élaborer et maintenir une culture encourageant une attitude positive envers le contrôle des risques et la vérification de la conformité au sein de l'établissement ainsi qu'un cadre de contrôle interne solide et exhaustif. Dans ce cadre, les lignes d'activité de l'établissement devraient être responsables de la gestion des risques auxquels elles sont exposées lorsqu'elles mènent leurs activités et elles devraient disposer de moyens de contrôle visant à garantir le respect des exigences internes et externes. Dans ce cadre, les établissements devraient disposer de fonctions de contrôle interne disposant d'une autorité, d'un statut et d'un accès à l'organe de direction appropriés et suffisants pour remplir leur mission, ainsi que d'un cadre de gestion des risques.

127. Le cadre de contrôle interne de l'établissement concerné devrait être adapté sur une base individuelle à la particularité de son activité, sa complexité et les risques associés, en tenant compte du contexte du groupe. Les établissements concernés doivent organiser l'échange d'informations nécessaires de manière à garantir que chaque organe de direction, ligne d'activité et unité interne, y compris chaque fonction de contrôle interne, est en mesure d'exercer ses attributions. Cela signifie, par exemple, un échange nécessaire d'informations adéquates entre les lignes d'activité et la fonction de vérification de la conformité au niveau du groupe ainsi qu'entre les responsables des fonctions de contrôle interne au niveau du groupe et l'organe de direction de l'établissement.

128. Le cadre de contrôle interne devrait couvrir l'ensemble de l'organisation, y compris les responsabilités et les tâches de l'organe de direction, et les activités de toutes les lignes d'activité et unités internes, y compris les fonctions de contrôle interne, les activités externalisées et les canaux de distribution.

129. Le cadre de contrôle interne de l'établissement devrait garantir:

a. des opérations effectives et efficaces;

b. une conduite des affaires prudente;

c. une détection, une mesure et une atténuation adéquates des risques;

d. la fiabilité des informations financières et non financières déclarées tant à l'intérieur qu'à l'extérieur de l'établissement;

e. des procédures administratives et comptables saines; et

f. le respect de la législation, de la réglementation, des exigences prudentielles et des politiques, procédures, règles et décisions internes de l'établissement.

16 Mise en œuvre d'un cadre de contrôle interne

130. L'organe de direction devrait être responsable de la mise en place et du suivi de l'adéquation et de l'efficacité du cadre, des procédures et des mécanismes de contrôle interne ainsi que de la supervision de toutes les lignes d'activité et des unités internes, y compris les fonctions de contrôle interne (telles que les fonctions de gestion des risques, de vérification de la conformité et d'audit interne). Les établissements devraient mettre en place, maintenir et actualiser régulièrement des politiques, des mécanismes et des procédures de contrôle interne écrits adéquats, qui devraient être approuvés par l'organe de direction.

131. L'établissement devrait être doté d'un processus de prise de décisions clair, transparent et documenté et prévoir une répartition des responsabilités et de l'autorité claire au sein de son cadre de contrôle interne, y compris ses lignes d'activité, unités internes et fonctions de contrôle interne.

132. Les établissements devraient communiquer ces politiques, mécanismes et procédures à l'ensemble du personnel et chaque fois que des modifications significatives y sont apportées.

133. Lorsqu'ils mettent en œuvre le cadre de contrôle interne, les établissements devraient prévoir une séparation appropriée des attributions, par exemple, en confiant à des personnes différentes les activités en conflit lors du traitement des transactions ou de la prestation de services ou en confiant à des personnes différentes les responsabilités en matière de surveillance et de déclaration pour les activités en conflit, et mettre en place des barrières pour empêcher la communication de l'information, par exemple par le cloisonnement physique de certains services.

134. Les fonctions de contrôle interne devraient vérifier que les politiques, les mécanismes et les procédures énoncés dans le cadre de contrôle interne sont correctement mis en œuvre dans leurs domaines de compétence respectifs.

135. Les fonctions de contrôle interne devraient régulièrement soumettre des rapports écrits à l'organe de direction concernant les déficiences majeures détectées. Ces rapports devraient inclure, pour chaque nouvelle déficience majeure détectée, les risques pertinents concernés, une analyse d'impact, des recommandations et des mesures correctives à adopter. L'organe de direction devrait donner suite aux constatations des fonctions de contrôle interne de manière efficace et en temps opportun, et exiger des mesures correctives adéquates. Une

procédure formelle de suivi des constatations et des mesures correctives adoptées devrait être mise en place.

17 Cadre de gestion des risques

136. Dans le contexte du cadre de contrôle interne global, les établissements devraient être dotés d'un cadre de gestion des risques holistique à l'échelle de l'établissement englobant toutes leurs lignes d'activité et unités internes, y compris les fonctions de contrôle interne, reconnaissant pleinement la substance économique de toutes leurs expositions au risque. Le cadre de gestion des risques devrait permettre à l'établissement d'arrêter des décisions pleinement éclairées sur la prise de risque. Le cadre de gestion des risques devrait inclure les risques de bilan et de hors bilan ainsi que les risques avérés et les risques futurs auxquels l'établissement peut être exposé. Les risques devraient être évalués selon des approches ascendante et descendante, au sein des lignes d'activité et entre celles-ci, en utilisant une terminologie cohérente et des méthodologies compatibles dans l'ensemble de l'établissement et aux niveaux consolidé ou sous-consolidé. Tous les risques pertinents devraient être compris dans le cadre de gestion des risques en tenant dûment compte des risques tant financiers que non financiers, y compris les risques de crédit, de marché, de liquidité, de concentration, opérationnel, informatique, de réputation, juridique, de conduite, de conformité et stratégique.

137. Le cadre de gestion des risques de l'établissement devrait comprendre des politiques, des procédures, des limites de risque et des mécanismes de maîtrise du risque lui permettant de détecter, de mesurer ou d'évaluer, de contrôler, de gérer, d'atténuer et de déclarer, de manière adéquate, continue et en temps utile, les risques aux niveaux des lignes d'activité, de l'établissement et aux niveaux consolidé ou sous-consolidé.

138. Le cadre de gestion des risques de l'établissement devrait fournir une orientation spécifique sur la mise en œuvre de ses stratégies. Cette orientation devrait, lorsque cela est approprié, fixer et maintenir des limites internes cohérentes par rapport à l'appétit pour le risque de l'établissement et adaptées en vue de son fonctionnement sain, de sa solidité financière, de son assise financière et de ses objectifs stratégiques. Le profil de risque de l'établissement devrait être maintenu dans ces limites fixées. Le cadre de gestion des risques devrait garantir que, lorsque surviennent des violations des limites de risque, il existe une procédure définie pour les communiquer aux niveaux hiérarchiques supérieurs et y répondre dans le cadre d'une procédure de suivi appropriée.

139. Le cadre de gestion des risques devrait faire l'objet d'un examen indépendant interne, réalisé, par exemple, par la fonction d'audit interne, et être régulièrement réévalué par rapport au profil d'appétit pour le risque de l'établissement, compte tenu des informations transmises par la fonction de gestion des risques et, s'il a été instauré, le comité des risques. Parmi les facteurs qui devraient être examinés figurent les événements internes et externes, y compris l'évolution du bilan et des recettes; l'éventuel accroissement de la complexité des activités de l'établissement, de son profil de risque ou de sa structure opérationnelle; le développement

géographique; les fusions et les acquisitions; et la commercialisation de nouveaux produits ou la mise en œuvre de nouvelles lignes d'activité.

140. Lorsqu'il détecte et mesure ou évalue les risques, l'établissement devrait élaborer des méthodologies appropriées, y compris des outils tant prospectifs que rétrospectifs. Les méthodologies devraient permettre d'agréger les expositions aux risques dans toutes les lignes d'activité et contribuer à identifier les concentrations de risques. Les outils devraient inclure l'évaluation du profil de risque avéré par rapport à l'appétit pour le risque de l'établissement ainsi que la détection et l'évaluation d'expositions potentielles à des risques et des tensions dans une série de circonstances défavorables hypothétiques par rapport à la capacité à prendre des risques de l'établissement. Les outils devraient fournir des informations sur tout ajustement du profil de risque éventuellement nécessaire. Les établissements devraient faire des hypothèses dûment conservatrices lorsqu'ils élaborent des scénarios de résistance.

141. Les établissements devraient tenir compte du fait que les résultats des méthodologies d'évaluation quantitative, y compris les tests de résistance, sont extrêmement dépendants des limites et des hypothèses des modèles (y compris la gravité et la durée du choc et les risques sous-jacents). Par exemple, des résultats faisant état d'un rendement très élevé du capital économique peuvent être imputables à une faiblesse du modèle (par exemple, l'exclusion de certains risques pertinents) plutôt qu'à une stratégie supérieure ou à l'exécution irréprochable d'une stratégie de la part de l'établissement. Par conséquent, la détermination du niveau de risque pris ne devrait pas reposer que sur des informations quantitatives ou des résultats obtenus au moyen de modèles; elle devrait également comprendre une approche qualitative (y compris un jugement d'expert et une analyse critique). Il convient de prendre en considération de manière appropriée les tendances et les données pertinentes du contexte macroéconomique afin d'identifier leur incidence potentielle sur les expositions et les portefeuilles.

142. La responsabilité finale de l'évaluation des risques appartient uniquement à l'établissement, qui, en conséquence, devrait évaluer de manière critique les risques auxquels il est exposé et ne pas s'appuyer exclusivement sur des évaluations externes. Par exemple, l'établissement devrait valider un modèle de risque qu'il a acheté et l'ajuster à ses propres circonstances spécifiques pour garantir que le modèle détecte et analyse le risque de manière précise et exhaustive.

143. Les établissements devraient être pleinement conscients des limites des modèles et des mesures et utiliser des outils d'évaluation des risques tant quantitatifs que qualitatifs (y compris le jugement d'expert et l'analyse critique).

144. Outre leurs propres évaluations, les établissements peuvent utiliser des évaluations des risques externes (y compris des notations de crédit externes ou des modèles de risque acquis en externe). Les établissements devraient être pleinement conscients de la portée exacte de ces évaluations et de leurs limites.

145. Des mécanismes de déclaration réguliers et transparents devraient être établis afin que l'organe de direction, son comité des risques, lorsqu'il a été instauré, et l'ensemble des unités concernées de l'établissement reçoivent en temps utile des rapports précis, concis, compréhensibles et judicieux, et puissent partager des informations pertinentes sur la détection, la mesure ou l'évaluation, le suivi et la gestion des risques. Le cadre de déclaration devrait être bien défini et documenté.

146. Une communication efficace et la connaissance des risques ainsi que de la stratégie en matière de risque sont essentielles pour l'ensemble du processus de gestion des risques, y compris les procédures d'examen et de prise de décisions, et contribuent à prévenir les décisions susceptibles d'accroître insidieusement les risques. Une déclaration efficace des risques exige une évaluation et une communication internes correctes de la stratégie en matière de risque et des données pertinentes en la matière (par exemple, expositions et indicateurs de risque clés), tant sur un plan horizontal, dans l'ensemble de l'établissement, qu'en amont et en aval de la chaîne de gestion.

18 Nouveaux produits et changements significatifs[24]

147. L'établissement devrait disposer d'une politique bien documentée de validation des nouveaux produits (PVNP), approuvée par l'organe de direction, axée sur l'ouverture de nouveaux marchés, la commercialisation de nouveaux produits et services et l'introduction de changements significatifs dans les offres existantes, ainsi que les transactions exceptionnelles. La politique devrait comprendre en outre les modifications significatives des processus (par exemple, les nouveaux dispositifs d'externalisation) et systèmes associés (par exemple, les processus de changements informatiques). La PVNP devrait garantir que les produits et les changements approuvés sont cohérents avec la stratégie en matière de risque et l'appétit pour le risque de l'établissement et les limites correspondantes ou que les révisions nécessaires sont réalisées.

148. Les changements significatifs ou les transactions exceptionnelles peuvent inclure les fusions et acquisitions, y compris les conséquences potentielles d'une vigilance insuffisante pour détecter les risques et les passifs résultant de ou survenant après la fusion; la mise en place de structures (par exemple, nouvelles filiales ou entités ad hoc); nouveaux produits; changements apportés aux systèmes ou au cadre ou procédures de gestion des risques; et changements apportés à l'organisation de l'établissement.

149. L'établissement devrait disposer de procédures spécifiques pour évaluer la conformité avec ces politiques, en tenant compte des informations fournies par la fonction de gestion des risques. Celles-ci devraient inclure une évaluation préalable systématique et un avis documenté de la part de la fonction de vérification de la conformité pour les nouveaux produits ou les changements significatifs apportés aux produits existants.

[24] Voir également orientations de l'ABE sur les modalités de gouvernance et de surveillance des produits bancaires de détail, disponibles à l'adresse https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products (fournir le lien vers la version française).

150. La PVNP de l'établissement devrait englober les aspects à prendre en considération avant que la décision ne soit prise de s'engager sur de nouveaux marchés, de commercialiser de nouveaux produits, de mettre en œuvre un nouveau service ou d'apporter des changements significatifs à des produits ou services existants. La PVNP devrait également inclure les définitions de «nouveau produit», «nouveau marché», «nouvelle activité» et «changements significatifs» telles qu'elles doivent être utilisées dans l'organisation et par les fonctions internes associées au processus de prise de décisions.

151. La PVNP devrait définir les principales questions à examiner avant qu'une décision ne soit arrêtée. Celles-ci comprennent notamment la conformité avec la réglementation, la comptabilité, les modèles tarifaires, l'incidence sur le profil de risque, l'adéquation des fonds propres et la rentabilité, l'allocation de ressources adéquates au front office, au back office et au middle office, ainsi que la disponibilité d'outils internes adéquats et de connaissances techniques suffisantes pour comprendre et contrôler les risques afférents. La décision de lancer une nouvelle activité devrait spécifier clairement la ligne d'activité concernée et les personnes qui en sont responsables. Une nouvelle activité ne devrait pas être entreprise avant que les ressources adéquates pour comprendre et gérer les risques afférents ne soient disponibles.

152. La fonction de gestion des risques et la fonction de vérification de la conformité devraient être associées à la validation des nouveaux produits ou des changements significatifs apportés aux produits, processus et systèmes existants. Leur contribution devrait inclure une évaluation complète et objective des risques engendrés par les nouvelles activités selon différents scénarios, de toute lacune potentielle dans les cadres de gestion des risques et de contrôle interne de l'établissement, ainsi que de la capacité de l'établissement à gérer efficacement tout nouveau risque. La fonction de gestion des risques devrait également avoir une vue d'ensemble claire de la mise sur le marché de nouveaux produits (ou des changements significatifs apportés à des produits; processus et systèmes existants) dans les différents portefeuilles et branches d'activité et le pouvoir d'exiger que l'introduction de changements dans les offres existantes soit soumise à la procédure formelle de la PVNP.

19 Fonctions de contrôle interne

153. Les fonctions de contrôle interne devraient comprendre une fonction de gestion des risques (voir section 20), une fonction de vérification de la conformité (voir section 21) et une fonction d'audit interne (voir section 22). Les fonctions de gestion des risques et de vérification de la conformité devraient être contrôlées par la fonction d'audit interne.

154. Les tâches opérationnelles des fonctions de contrôle interne peuvent être externalisées, en tenant compte des critères de proportionnalité énoncés au titre I, à l'établissement consolidant ou à une autre entité au sein ou en dehors du groupe avec l'accord des organes de direction des établissements concernés. Même lorsque les tâches opérationnelles de contrôle interne sont externalisées, en tout ou en partie, le responsable de la fonction de

contrôle interne concernée et l'organe de direction demeurent responsables de ces activités et du maintien d'une fonction de contrôle interne dans l'établissement.

19.1 Responsables des fonctions de contrôle interne

155. Les responsables des fonctions de contrôle interne devraient être mis en place à un niveau hiérarchique adéquat conférant au responsable de la fonction de contrôle l'autorité et le statut appropriés nécessaires pour s'acquitter de leurs responsabilités. Nonobstant la responsabilité globale de l'organe de direction, les responsables des fonctions de contrôle interne devraient être indépendants des lignes d'activité ou des unités qu'ils contrôlent. À cet effet, les responsables des fonctions de gestion des risques, de vérification de la conformité et d'audit interne devraient rendre des comptes et répondre de leurs actes directement à l'organe de direction et leurs performances devraient être réexaminées par l'organe de direction.

156. Si nécessaire, les responsables de fonctions de contrôle interne devraient être en mesure d'avoir accès et de rendre des comptes directement à l'organe de direction dans sa fonction de surveillance afin de faire part de leurs préoccupations et d'alerter la fonction de surveillance, le cas échéant, lorsque des évolutions particulières affectent ou sont susceptibles d'affecter l'établissement. Cela ne devrait pas empêcher les responsables de fonctions de contrôle interne de rendre des comptes également selon les voies hiérarchiques traditionnelles.

157. Les établissements devraient disposer de procédures documentées pour pourvoir le poste de responsable d'une fonction de contrôle interne et pour le décharger de ses responsabilités. En tout état de cause, les responsables des fonctions de contrôle interne ne devraient pas – et, conformément à l'article 76, paragraphe 5, de la directive 2013/36/UE, le responsable de la fonction de gestion des risques ne doit pas – être démis de leurs fonctions sans l'accord préalable de l'organe de direction dans l'exercice de sa fonction de surveillance. Dans les établissements ayant une importance significative, les autorités compétentes devraient être rapidement informées de la nomination et des principales raisons de la révocation d'un responsable d'une fonction de contrôle interne.

19.2 Indépendance des fonctions de contrôle interne

158. Pour que les fonctions de contrôle interne soient considérées comme indépendantes, les conditions suivantes devraient être remplies:

a. leur personnel ne s'acquitte d'aucune tâche opérationnelle relevant du champ d'application des activités que les fonctions de contrôle interne ont pour mission de surveiller et de contrôler;

b. elles sont séparées sur le plan organisationnel des activités qu'elles sont chargées de surveiller et de contrôler;

c. nonobstant la responsabilité globale des membres de l'organe de direction pour l'établissement, le responsable d'une fonction de contrôle interne ne devrait pas être subordonné à une personne responsable de la gestion des activités que la fonction de contrôle interne surveille et contrôle; et

d. la rémunération du personnel des fonctions de contrôle interne ne devrait pas être liée à la performance des activités que celles-ci surveillent et contrôlent, et ne devrait pas nuire à son objectivité de quelqu'autre manière que ce soit[25].

19.3 Fonctions de contrôle interne communes

159. En tenant compte des critères de proportionnalité énoncés au titre I, la fonction de gestion des risques et la fonction de vérification de la conformité peuvent être fusionnées. La fonction d'audit interne ne devrait pas être fusionnée avec une autre fonction de contrôle interne.

19.4 Ressources des fonctions de contrôle interne

160. Les fonctions de contrôle interne devraient disposer de ressources suffisantes. Elles devraient disposer d'un personnel qualifié en nombre suffisant (tant au niveau de l'entreprise mère qu'à celui des filiales). Le personnel devrait toujours demeurer suffisamment qualifié et devrait bénéficier des formations nécessaires.

161. Les fonctions de contrôle interne devraient également disposer de systèmes informatiques et d'assistance et avoir accès aux informations internes et externes nécessaires pour assumer leurs responsabilités. Elles devraient avoir accès à toutes les informations nécessaires concernant toutes les lignes d'activité et les filiales pertinentes impliquant un risque, notamment celles susceptibles de créer des risques significatifs pour les établissements.

20 Fonction de gestion des risques

162. Les établissements devraient instaurer une fonction de gestion des risques (FGR) couvrant l'ensemble de l'établissement. La FGR devrait disposer d'une autorité, d'un statut et de ressources suffisants, compte tenu des critères de proportionnalité énoncés au titre I, pour mettre en œuvre les politiques en matière de risque et le cadre de gestion des risques comme prévu à la section 17.

163. Si nécessaire, la FGR devrait avoir un accès direct à l'organe de direction dans sa fonction de surveillance et à ses comités, lorsqu'ils sont instaurés, y compris notamment le comité des risques.

164. La FGR devrait avoir accès à toutes les lignes d'activité et autres unités internes susceptibles de créer des risques, ainsi qu'aux filiales et aux parties liées pertinentes.

[25] Voir également orientations de l'ABE sur les politiques de rémunération saines, disponibles à l'adresse https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies (fournir le lien vers la version anglaise).

165. Le personnel de la FGR devrait disposer de connaissances, de compétences et d'une expérience suffisantes en rapport avec les techniques et procédures de gestion des risques ainsi que les marchés et les produits et devrait avoir accès à une formation régulière.

166. La FGR devrait être indépendante des lignes d'activité et des unités dont elle contrôle les risques mais elle ne devrait pas être empêchée d'interagir avec celles-ci. Les interactions entre les fonctions opérationnelles et la FGR devraient permettre la réalisation de l'objectif de l'ensemble du personnel de l'établissement chargé de la responsabilité de la gestion des risques.

167. La FGR devrait constituer un élément central de l'organisation de l'établissement et être structurée de manière à pouvoir mettre en œuvre des politiques en matière de risque et contrôler le cadre de gestion des risques. La FGR devrait jouer un rôle essentiel pour garantir que l'établissement dispose de processus efficaces de gestion des risques. La FGR devrait participer activement à la prise de toutes les décisions concernant la gestion des risques significatifs.

168. Les établissements ayant une importance significative peuvent envisager de mettre en place une FGR dédiée pour chaque ligne d'activité d'importance significative. Cependant, il devrait exister une FGR centrale, y compris une FGR du groupe dans l'établissement consolidant, exprimant un point de vue holistique sur l'ensemble des risques à l'échelle de l'établissement et du groupe et garantissant le respect de la stratégie en matière de risque.

169. La FGR devrait fournir des informations, des analyses et des expertises indépendantes et pertinentes sur les expositions aux risques et formuler des conseils quant aux propositions et aux décisions en matière de risque adoptées par les lignes d'activité ou les unités internes et elle devrait informer l'organe de direction de leur cohérence avec l'appétit pour le risque et la stratégie en matière de risque de l'établissement. La FGR peut recommander des améliorations à apporter au cadre de gestion des risques, ainsi que des mesures correctives permettant de remédier à des violations des politiques, procédures et limites relatives aux risques.

20.1 Rôle de la FGR vis-à-vis de la stratégie en matière de risque et de la prise de décisions

170. La FGR devrait participer activement et à un stade précoce à l'élaboration de la stratégie de l'établissement en matière de risques et veiller à ce que l'établissement dispose de procédures efficaces de gestion des risques. La FGR devrait fournir à l'organe de direction toutes les informations pertinentes en matière de risques dont il a besoin pour déterminer le niveau d'appétit pour le risque de l'établissement. La FGR devrait évaluer la solidité et la durabilité de la stratégie en matière de risque et de l'appétit pour le risque. Elle devrait garantir que l'appétit pour le risque est dûment traduit par des limites de risque spécifiques. La FGR devrait également évaluer les stratégies en matière de risque des unités opérationnelles, y compris les objectifs proposés par les unités opérationnelles, et devrait être consultée avant l'adoption

d’une décision par l’organe de direction concernant les stratégies en matière de risque. Les objectifs devraient être plausibles et cohérents avec la stratégie en matière de risque de l’établissement.

171. La participation de la FGR aux processus de prise de décisions devrait garantir que les questions relatives aux risques sont dûment prises en considération. Cependant, les décisions prises devraient rester de la responsabilité des unités opérationnelles et des unités internes et, en dernier ressort, de l'organe de direction.

20.2 Rôle de la FGR en matière de changements significatifs

172. Conformément à la section 18, avant que des décisions relatives à des changements significatifs ou à des transactions exceptionnelles ne soient prises, la FGR devrait être associée à l'évaluation des incidences de ces changements et de ces transactions exceptionnelles sur le risque global auquel l'établissement et le groupe sont exposés et devrait rendre compte de ses constatations directement à l’organe de direction avant l’adoption d’une décision.

173. La FGR devrait évaluer dans quelle mesure les risques recensés pourraient porter préjudice à la capacité de l'établissement ou du groupe à gérer son profil de risque, sa liquidité et son assise financière saine dans des conditions normales et défavorables.

20.3 Le rôle de la FGR en matière de détection, de mesure, d’évaluation, de gestion, d’atténuation, de suivi et de déclaration des risques

174. La FGR devrait veiller à ce que tous les risques soient détectés, évalués, mesurés, suivis, gérés et dûment déclarés par les unités concernées de l’établissement.

175. La FGR devrait garantir que la détection et l’évaluation ne reposent pas uniquement sur des informations quantitatives ou des résultats de modèles et tenir également compte d’approches qualitatives. La FGR devrait tenir l’organe de direction informé des hypothèses utilisées dans les modèles et l’analyse des risques ainsi que des éventuelles lacunes des modèles et analyses des risques.

176. La FGR devrait s'assurer que les transactions avec des parties liées sont examinées et que les risques qu'elles comportent pour l'établissement sont recensés et dûment évalués.

177. La FGR devrait s'assurer que tous les risques recensés font l’objet d’un suivi efficace par les unités opérationnelles.

178. La FGR devrait suivre régulièrement le profil de risque avéré de l'établissement et le comparer à ses objectifs stratégiques et à son appétit pour le risque pour permettre à l'organe de direction de prendre des décisions dans le cadre de sa fonction exécutive et de les remettre en cause dans le cadre de sa fonction de surveillance.

179. La FGR devrait analyser les tendances et déceler les risques nouveaux ou émergents et les accroissements du risque liés à des changements de conditions et de circonstances. Elle devrait également réexaminer régulièrement les résultats en matière de risques avérés par rapport à des estimations antérieures (contrôles a posteriori), afin d'évaluer et d'améliorer la précision et l'efficacité du processus de gestion des risques.

180. La FGR devrait évaluer les moyens pouvant être mis en œuvre pour atténuer les risques. Les rapports présentés à l'organe de direction devraient comporter des propositions d'actions appropriées en vue d'atténuer les risques.

20.4 Rôle de la FGR en matière d'expositions non approuvées

181. La FGR devrait évaluer de manière indépendante toute violation de l'appétit pour le risque ou des limites de risque (y compris en déterminant son origine et en effectuant une analyse juridique et économique du coût réel de la suppression, de la réduction ou de la couverture de l'exposition par rapport au coût potentiel de son maintien). La FGR devrait informer les unités opérationnelles concernées et l'organe de direction et recommander des mesures correctives envisageables. La FGR devrait rendre des comptes directement à l'organe de direction dans sa fonction de surveillance lorsque la violation est significative, sans préjudice de l'obligation de la FGR de rendre des comptes à d'autres fonctions internes et comités.

182. La FGR devrait jouer un rôle essentiel pour garantir qu'une décision est prise au niveau approprié suite à une recommandation qu'elle a formulée, qu'elle est appliquée par les unités opérationnelles concernées et qu'elle est dûment notifiée à l'organe de direction et, lorsqu'il est instauré, au comité des risques.

20.5 Responsable de la fonction de gestion des risques

183. Le responsable de la FGR devrait être responsable de la fourniture d'informations complètes et compréhensibles sur les risques et de conseils à l'organe de direction, permettant à celui-ci de comprendre le profil de risque global de l'établissement. La même disposition s'applique au responsable de la FGR de l'établissement mère à l'égard de la situation consolidée.

184. Le responsable de la FGR devrait disposer de suffisamment d'expertise, d'indépendance et d'ancienneté pour remettre en question les décisions affectant l'exposition de l'établissement aux risques. Lorsque le responsable de la FGR n'est pas un membre de l'organe de direction, les établissements ayant une importance significative devraient nommer un responsable de la FGR indépendant n'ayant aucune responsabilité pour d'autres fonctions et rendant des comptes directement à l'organe de direction. Lorsqu'il n'est pas adéquat au regard de la taille de l'établissement de nommer une personne uniquement dédiée au rôle de responsable de la FGR, compte tenu du principe de proportionnalité énoncé au titre I, cette fonction peut être fusionnée avec celle du responsable de la fonction de vérification de la conformité ou être exercée par une autre personne titulaire d'un poste supérieur, à condition qu'il n'y ait pas de conflits d'intérêts entre les fonctions fusionnées. En tout état de cause, cette personne devrait

disposer d'une autorité, d'un statut et d'une indépendance suffisants (par exemple, responsable du service juridique).

185. Le responsable de la FGR devrait être en mesure de remettre en cause les décisions adoptées par la direction de l'établissement et son organe de direction et les motifs justifiant les objections devraient être formellement documentés. Si l'établissement souhaite accorder au responsable de la FGR un droit de veto sur certaines décisions (par exemple, une décision de crédit ou d'investissement ou la fixation d'une limite) adoptées à des niveaux inférieurs à celui de l'organe de direction, il devrait préciser la portée d'un tel droit de veto, les procédures d'escalade aux niveaux supérieurs ou de recours et les modalités de participation de l'organe de direction.

186. Les établissements devraient mettre en place des procédures renforcées pour l'approbation de décisions à propos desquelles le responsable de la FGR a exprimé une opinion défavorable. L'organe de direction dans sa fonction de surveillance devrait être en mesure de communiquer directement avec le responsable de la FGR sur des problématiques de risque importantes, y compris les évolutions qui peuvent ne pas être cohérentes avec l'appétit pour le risque et la stratégie en matière de risque de l'établissement.

21 Fonction de vérification de la conformité

187. Les établissements devraient mettre en place une fonction de vérification de la conformité permanente et efficace pour gérer le risque de conformité et nommer une personne responsable de cette fonction pour l'ensemble de l'établissement (le responsable de la conformité ou le directeur de la conformité).

188. Lorsqu'il n'est pas adéquat au regard de la taille de l'établissement de nommer une personne uniquement dédiée au rôle de responsable de la conformité, compte tenu du principe de proportionnalité énoncé au titre I, cette fonction peut être fusionnée avec celle du responsable de la FGR ou être exercée par une autre personne titulaire d'un poste supérieur, à condition qu'il n'y ait pas de conflits d'intérêts entre les fonctions fusionnées.

189. La fonction de conformité, y compris le responsable de conformité, devrait être indépendante des lignes d'activité et des unités internes qu'elle contrôle et disposer d'une autorité, d'un statut et de ressources suffisants. Compte tenu des critères de proportionnalité énoncés au titre I, cette fonction peut bénéficier de l'assistance de la FGR ou être fusionnée avec la FGR ou avec d'autres fonctions appropriées, par exemple, le service juridique ou les ressources humaines.

190. Le personnel de la fonction de vérification de la conformité devrait disposer de connaissances, de compétences et d'une expérience suffisantes en rapport avec la vérification de la conformité et les procédures pertinentes et devrait avoir accès à une formation régulière.

191. L'organe de direction dans sa fonction de surveillance devrait superviser la mise en œuvre d'une politique en matière de vérification de la conformité bien documentée, qui devrait être

communiquée à l'ensemble du personnel. Les établissements devraient mettre en place une procédure pour évaluer régulièrement les modifications de la législation et de la réglementation applicables à leurs activités.

192. La fonction de vérification de la conformité devrait fournir ses conseils à l'organe de direction sur les mesures à adopter en vue de garantir la conformité avec les lois, les règles, les règlements et les normes applicables et devrait évaluer l'incidence potentielle de tout changement apporté au cadre juridique ou réglementaire sur les activités de l'établissement et le cadre de vérification de la conformité.

193. La fonction de vérification de la conformité devrait veiller à ce que le contrôle de conformité soit réalisé par le biais d'un programme de contrôle de la conformité structuré et bien défini et à ce que la politique en matière de vérification de la conformité soit respectée. La fonction de vérification de la conformité devrait rendre des comptes à l'organe de direction et communiquer selon que de besoin avec la FGR sur le risque de conformité auquel l'établissement est exposé et sur sa gestion. La fonction de vérification de la conformité et la FGR devraient coopérer et échanger des informations le cas échéant afin de mener à bien leurs tâches respectives. Les conclusions de la fonction de vérification de la conformité devraient être prises en considération par l'organe de direction et la FGR dans les procédures de prise de décisions.

194. Conformément à la section 18 des présentes orientations, la fonction de vérification de la conformité devrait également vérifier, en étroite coopération avec la FGR et le service juridique, que les nouveaux produits et les nouvelles procédures sont conformes avec le cadre juridique actuel et, le cas échéant, les modifications connues qui seront apportées à la législation, la réglementation et les exigences prudentielles.

195. Les établissements devraient prendre les mesures appropriées pour éviter les comportements frauduleux, tant sur le plan interne que sur le plan externe, ainsi que les manquements à la discipline (par exemple, une infraction aux procédures internes ou un dépassement des limites).

196. Les établissements devraient veiller à ce que leurs filiales et leurs succursales adoptent des mesures visant à garantir que leurs opérations respectent le cadre légal et réglementaire local. Si le cadre légal et réglementaire local empêche l'application de procédures et de systèmes de vérification de la conformité plus stricts mis en œuvre par le groupe, notamment s'il empêche la divulgation et l'échange d'informations nécessaires entre entités au sein du groupe, les filiales et les succursales devraient informer le responsable de la conformité ou le directeur de la conformité de l'établissement consolidant.

22 Fonction d'audit interne

197. Les établissements devraient instaurer une fonction d'audit interne (FAI) indépendante et efficace, en tenant compte des critères de proportionnalité énoncés au titre I, et devraient

nommer une personne qui sera responsable de cette fonction dans l'ensemble de l'établissement. La FAI devrait être indépendante et disposer d'une autorité, d'un statut et de ressources suffisants. L'établissement devrait notamment veiller à ce que les qualifications des membres du personnel de la FAI et les ressources de la FAI, et plus précisément ses outils d'audit et ses méthodes d'analyse des risques, soient adéquats par rapport à la taille et aux lieux d'implantation de l'établissement ainsi qu'à la nature, l'échelle et la complexité des risques associés au modèle d'entreprise, aux activités, à la culture du risque et à l'appétit pour le risque de l'établissement.

198. La FAI devrait être indépendante des activités contrôlées. La FAI ne devrait donc pas être fusionnée avec d'autres fonctions.

199. En adoptant une approche fondée sur les risques, la FAI devrait examiner de manière indépendante et fournir une assurance objective de la conformité de toutes les activités et unités d'un établissement, y compris les activités externalisées, avec les politiques et les procédures de l'établissement et avec les exigences externes. Toute entité au sein du groupe devrait relever de la compétence de la FAI.

200. La FAI ne devrait pas participer à la conception, la sélection, la mise en place et la mise en œuvre de politiques, mécanismes et procédures de contrôle interne spécifiques ainsi que de limites de risque. Toutefois, cela ne devrait pas empêcher l'organe de direction dans sa fonction exécutive de demander des informations à l'audit interne sur des questions liées au risque, aux contrôles internes et à la conformité avec les règles applicables.

201. La FAI devrait évaluer si le cadre de contrôle interne de l'établissement, tel qu'énoncé à la section 15, est effectif et efficace. La FAI devrait notamment évaluer:

a. l'adéquation du cadre de gouvernance de l'établissement;

b. si les politiques et les procédures existantes demeurent adéquates et respectent les exigences juridiques et réglementaires ainsi que l'appétit pour le risque et la stratégie en matière de risque de l'établissement;

c. la conformité des procédures avec la législation et les réglementations applicables et avec les décisions de l'organe de direction;

d. si les procédures sont mises en œuvre de manière appropriée et efficace (par exemple, conformité des transactions, niveau de risque réellement subi etc.); et

e. l'adéquation, la qualité et l'efficacité des contrôles réalisés et les rapports rendus par les unités opérationnelles de la première ligne de défense et les fonctions de gestion des risques et de vérification de la conformité.

202. La FAI devrait en particulier vérifier l'intégrité des processus garantissant la fiabilité des méthodes et techniques de l'établissement ainsi que des hypothèses et les sources d'information utilisées pour ses modèles internes (par exemple, pour établir des modèles de risque et effectuer des mesures comptables). Elle devrait également évaluer la qualité et l'utilisation des outils qualitatifs de détection et d'évaluation des risques et les mesures d'atténuation des risques adoptées.

203. La FAI devrait avoir le libre accès à l'échelle de l'établissement à tous les dossiers, documents, informations et immeubles de l'établissement. Cela devrait inclure l'accès aux systèmes de gestion des informations et aux procès-verbaux de tous les comités et organes de prise de décisions.

204. La FAI devrait respecter les normes professionnelles nationales et internationales. Les normes établies par l'Institut des auditeurs internes offrent un exemple des normes professionnelles susmentionnées.

205. Le travail d'audit interne devrait être réalisé conformément à un plan d'audit et à un programme d'audit détaillé, suivant une approche fondée sur les risques.

206. Un plan d'audit interne devrait être établi au moins une fois par an sur la base des objectifs annuels en matière de contrôles d'audit interne. Le plan d'audit interne devrait être approuvé par l'organe de direction.

207. Toutes les recommandations en matière d'audit devraient être soumises à une procédure formelle de suivi par le niveau de gestion approprié, afin de garantir qu'elles sont prises en compte de manière efficace et en temps utiles et de rendre des comptes à ce sujet.

Titre VI – Gestion de la continuité des activités

208. Les établissements devraient mettre en place un plan de gestion saine de la continuité de leurs activités, afin de garantir leur capacité à fonctionner sans interruption et de limiter les pertes en cas de perturbation grave de leurs activités.

209. Les établissements peuvent instaurer une fonction indépendante spécifique de continuité des activités, par exemple dans le cadre de la FGR[26].

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

[26] Voir également article 312 du règlement (UE) n° 575/2013.

réduire la probabilité de ces incidents ou à transférer leurs conséquences financières à des tiers (par exemple, en souscrivant une assurance).

211. Afin de mettre en place un plan de gestion raisonnable de la continuité de ses activités, un établissement devrait analyser avec soin son exposition à des perturbations graves de ses activités et évaluer (sur le plan tant quantitatif que qualitatif) leurs incidences potentielles au moyen d'une analyse interne et/ou externe de données et de scénarios. Cette analyse devrait couvrir l'ensemble des lignes d'activités et des unités internes, y compris la FGR, et tenir compte de leur interdépendance. Les résultats de l'analyse devraient contribuer à la définition des priorités et des objectifs de l'établissement en matière de reprise des activités.

212. Sur la base de l'analyse susmentionnée, l'établissement devrait mettre en place:

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

b. des plans de rétablissement des ressources critiques permettant à l'établissement de rétablir ses procédures opérationnelles ordinaires dans un délai approprié. Tout risque résiduel lié à des perturbations potentielles des activités devrait être compatible avec l'appétit pour le risque de l'établissement.

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

Titre VII – Transparence

214. Les stratégies, les politiques et les procédures devraient être communiquées à tout le personnel concerné, dans l'ensemble de l'établissement. Les membres du personnel de l'établissement devraient comprendre et respecter les politiques et procédures liées à leurs missions et responsabilités.

215. En conséquence, l'organe de direction devrait informer les membres du personnel concerné des stratégies et des politiques de l'établissement de manière claire et cohérente et maintenir ces informations à jour, au moins au niveau nécessaire pour leur permettre d'accomplir les tâches qui leur incombent. Cette information peut être transmise par le biais d'orientations écrites, de manuels ou d'autres supports.

216. Lorsque les autorités compétentes exigent, au titre de l'article 106, paragraphe 2, de la directive 2013/36/UE, des entreprises mères qu'elles publient une fois par an une description de leur structure juridique, ainsi que de la structure de gouvernance et organisationnelle de leur groupe d'établissements, les informations devraient comprendre toutes les entités au sein de la structure de groupe au sens de la directive 2013/34/UE[27], par pays.

217. Cette publication devrait inclure à tout le moins:

a. Une vue d'ensemble de l'organisation interne des établissements et de la structure de groupe au sens de la directive 2013/34/UE et des changements apportés à celles-ci, y compris les principales voies hiérarchiques et responsabilités;

b. les changements significatifs intervenus depuis la dernière publication et la date du changement significatif;

c. les nouvelles structures juridiques, de gouvernance ou organisationnelles;

d. des informations sur la structure, l'organisation et les membres de l'organe de direction, y compris le nombre de ses membres et le nombre de ceux qualifiés d'indépendants, précisant le sexe et la durée du mandat de chaque membre de l'organe de direction;

e. les principales responsabilités de l'organe de direction;

f. une liste des comités de l'organe de direction dans sa fonction de surveillance et leur composition;

g. une vue d'ensemble de la politique en matière de conflits d'intérêts applicable aux établissements et à l'organe de direction;

h. une vue d'ensemble du cadre de contrôle interne; et

i. une vue d'ensemble du cadre de gestion de la continuité des activités.

Annexe I – Aspects à prendre en considération lors de l'élaboration d'une politique de gouvernance interne

[27] Directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises, modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (JO L 182 du 29.6.2013, p. 19).

Conformément au titre III, les établissements devraient accorder de l'attention aux aspects suivants lorsqu'ils documentent des politiques et des dispositifs de gouvernance interne:

1. Structure de l'actionnariat
2. Structure du groupe, le cas échéant (structure juridique et opérationnelle)
3. Composition et fonctionnement de l'organe de direction
   a) critères de sélection
   b) nombre, durée du mandat, rotation, âge
   c) membres indépendants de l'organe de direction
   d) membres de l'organe de direction exerçant des fonctions exécutives
   e) membres de l'organe de direction n'exerçant pas de fonctions exécutives
   f) répartition interne des tâches, le cas échéant
4. Structure de gouvernance et organigramme (avec incidence sur le groupe, le cas échéant)
   a) comités spécialisés
      i. composition
      ii. fonctionnement
   b) comité exécutif, pour autant qu'il ait été institué
      i. composition
      ii. fonctionnement
5. Titulaires de postes clés
   a) responsable de la fonction de gestion des risques
   b) responsable de la fonction de vérification de la conformité
   c) responsable de la fonction d'audit interne
   d) directeur financier
   e) autres titulaires de postes clés
6. Cadre de contrôle interne
   a) description de chaque fonction, y compris son organisation, ses ressources, son statut et son autorité
   b) description du cadre de gestion des risques, y compris la stratégie en matière de risque
7. Structure organisationnelle (avec incidence sur le groupe, le cas échéant)
   a) structure opérationnelle, lignes d'activité et répartition de compétences et de responsabilités
   b) externalisation
   c) gamme de produits et de services

d) portée géographique de l’activité

e) prestation gratuite de services

f) succursales

g) filiales, coentreprises etc.

h) utilisation de centres extraterritoriaux

8. Code de conduite et de comportement (avec incidence sur le groupe, le cas échéant)

a) objectifs stratégiques et valeurs de l’entreprise

b) codes et règles internes, politique en matière de prévention

c) politique en matière de conflits d'intérêts

d) dénonciation des dysfonctionnements

9. Statut de la politique en matière de gouvernance interne, avec date

a) élaboration

b) dernière modification

c) dernière évaluation

d) approbation par l’organe de direction.