

EBA/GL/2021/05

2 juillet 2021

Projet d'orientations

en matière de gouvernance interne

1. Obligations de conformité et de déclaration

Statut des présentes orientations

1. Les présentes orientations sont publiées conformément à l'article 16 du règlement (UE) n° 1093/2010¹. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes et les institutions financières, y compris les établissements, mettent tout en œuvre pour respecter ces orientations.
2. Les orientations exposent l'avis de l'ABE sur les 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 lorsqu'elles 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 les présentes orientations, ou indiquer les raisons du non-respect des orientations, le cas échéant, avant le (05.12.2021). En l'absence de toute notification avant cette date, l'ABE considérera que l'autorité compétente ne s'est pas mise en conformité. Les notifications sont à adresser à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site internet de l'ABE en indiquant en objet «EBA/GL/2021/05». Les notifications devraient être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom de leur autorité compétente. Toute modification du statut de conformité aux orientations doit également être signalée à l'ABE.
4. Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010.

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

2. Objet, champ d'application et définitions

Objet

5. Les présentes orientations précisent les dispositifs, processus et mécanismes de gouvernance interne que les établissements soumis à la directive 2013/36/UE² et les entreprises d'investissement soumises au titre VII de ladite directive, en application de l'article 1, paragraphes 2 et 5, du règlement (UE) 2019/2033, devraient mettre en œuvre conformément à l'article 74, paragraphe 1, de la directive 2013/36/UE afin de garantir leur gestion efficace et prudente.

Destinataires

Les présentes orientations sont destinées aux autorités compétentes au sens de l'article 4, paragraphe 2, point i), du règlement (UE) n° 1093/2010, ainsi qu'aux établissements financiers, au sens de l'article 4, paragraphe 1, dudit règlement, qui sont soit des établissements aux fins de l'application de la directive 2013/36/UE, tels que définis à l'article 3, paragraphe 1, point 3), de ladite directive, eu égard également à l'article 3, paragraphe 3, de ladite directive, soit des entreprises d'investissement soumises au titre VII de la directive 2013/36/UE en application de l'article 1, paragraphes 2 et 5, du règlement (UE) 2019/2033 (« établissements »).

Champ d'application

6. Les présentes orientations s'appliquent en relation avec les dispositifs 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 de tous les risques³ auxquels ils sont ou pourraient être exposés, ainsi que le cadre de contrôle interne.
7. Les orientations visent à prendre en compte l'ensemble des structures de conseil d'administration existantes sans en privilégier aucune 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 du conseil d'administration 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)

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 du 27.6.2013, p. 338).

³ Dans les présentes orientations, toute référence faite aux risques devrait inclure les risques de blanchiment de capitaux et de financement du terrorisme.

et 8), de la directive 2013/36/UE, devrait être compris comme ayant une fonction de gestion (exécutive) et une fonction de surveillance (non exécutive)⁴.

8. Les termes « organe de direction dans sa fonction exécutive » et « organe de direction dans sa fonction de surveillance » sont utilisés tout au long des présentes orientations sans se référer à une quelconque structure de gouvernance spécifique et les références aux fonctions de gestion (exécutive) ou de surveillance (non exécutive) devraient être interprétées comme s'appliquant aux organes ou aux 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 des sociétés national et préciser, le cas échéant, l'organe ou les membres de l'organe de direction à qui ces orientations devraient s'appliquer.
9. Dans les États membres où l'organe de direction délègue la totalité ou une partie des 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 de gestion 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.
10. Dans les États membres où certaines responsabilités sont exercées directement par les actionnaires, les membres ou les propriétaires de l'établissement, et non pas 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.
11. Les définitions de « directeur général », « directeur financier » et « 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.
12. 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.

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

Définitions

13. Sauf indication contraire, les termes utilisés et définis dans la directive 2013/36/UE et le règlement (UE) n° 575/2013 ont la même signification dans les orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

Actionnaire	désigne une personne propriétaire d'actions d'un établissement ou, selon la forme juridique de l'établissement, d'autres propriétaires ou membres de l'établissement.
Appétit pour le risque	désigne 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	désigne 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.
Consolidation prudentielle	désigne 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 ⁵ .
Culture du risque	désigne 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.
Directeur financier	désigne la personne globalement en charge de la gestion de l'ensemble des activités suivantes : gestion des ressources financières, planification financière et information financière.
Directeur général	désigne la personne en charge de la gestion et de la direction de l'ensemble des activités d'un établissement.
Écart de rémunération entre les hommes et les femmes	désigne la différence entre la rémunération horaire brute moyenne des hommes et celle des femmes, exprimée en pourcentage de la rémunération horaire brute moyenne des hommes.

⁵ Voir également la NTR sur la consolidation prudentielle, à l'adresse https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf

Établissement consolidant	désigne 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	désigne les 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, d'autres établissements déterminés par l'autorité compétente ou le droit national, 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 coté	désigne les établissements dont les instruments financiers sont admis à la négociation 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 ⁶ .
Fonction de direction	désigne un poste de membre de l'organe de direction d'un établissement ou d'une autre entité juridique.
Personnel	désigne l'ensemble des employés d'un établissement et des filiales entrant dans son périmètre de consolidation, y compris les filiales ne relevant pas de la directive 2013/36/UE, ainsi que l'ensemble des membres de l'organe de direction dans sa fonction de gestion et dans sa fonction de surveillance.
Responsables de fonctions de contrôle interne	désigne les personnes du 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	désigne les 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. Il s'agit notamment des responsables de fonctions de contrôle interne et le directeur financier, si ceux-ci ne sont pas membres de l'organe de direction, et, s'ils sont détectés 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 inclure 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.

⁶ 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).

3. Mise en œuvre

Date d'application

14. Les présentes orientations actualisées s'appliquent à compter du 31 décembre 2021.

Abrogation

15. Les orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11) du 26 septembre 2017 sont abrogées à compter du 31 décembre 2021.

4. Orientations

Titre I – Proportionnalité

16. 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 et dispositions réglementaires soient efficacement atteints.
17. 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. Les établissements devraient toutefois noter que la taille ou l'importance systémique d'un établissement peut ne pas refléter à elle seule la mesure dans laquelle cet établissement est exposé à des risques.
18. Aux fins de l'application du principe de proportionnalité et afin de garantir une mise en œuvre adéquate des exigences réglementaires et des présentes orientations, les établissements et les autorités compétentes devraient tenir compte de tous les aspects suivants:
 - a. la taille, déterminée par le total du 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 ou non 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 également l'annexe 1 de la directive 2013/36/UE et l'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 de ses activités et sa structure organisationnelle;
- 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 processus de contrôle et d'évaluation prudentiels.
- i. la structure de propriété et la structure de financement de l'établissement;
- j. le type de clientèle (par exemple de détail, entreprises, institutions, petites entreprises, entités publiques) et la complexité des produits ou contrats;
- k. les fonctions externalisées et les canaux de distribution;
- l. les systèmes informatiques existants, y compris les systèmes de continuité et les fonctions externalisées dans ce domaine; et
- m. le fait que l'établissement tombe dans le champ d'application de la définition d'un « établissement de petite taille et non complexe » ou d'un « établissement de grande taille » à l'article 4, paragraphe 1, points 145 et 146, du règlement (UE) n° 575/2013

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

1 Rôle et responsabilités de l'organe de direction

- 19. 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. Il définit et supervise la mise en œuvre, au sein de l'établissement, de dispositifs de gouvernance qui garantissent la gestion efficace et prudente de l'établissement, et rend des comptes à cet égard.
- 20. 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 approuvé par l'organe de direction. Tous les membres de l'organe de direction devraient avoir une connaissance sans faille 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 de ses comités.
- 21. 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 se fournir suffisamment d'informations leur permettant d'exercer leurs rôles respectifs. Afin que des contre-pouvoirs appropriés soient en place, 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.

22. 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, l'appétit pour le risque de l'établissement, 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, tel que défini au titre V, qui :
 - i. inclut 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 ;
 - ii. garantit la conformité aux exigences réglementaires applicables dans le contexte de la prévention du blanchiment de capitaux et le financement du terrorisme ;
- d. les montants, la nature et la répartition des capitaux internes et des fonds propres réglementaires suffisant à 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 de rémunération énoncés aux articles 92 à 95 de la directive 2013/36/UE et dans les orientations de l'ABE sur les politiques de rémunération saines au titre de l'article 74, paragraphe 3, et de l'article 75, paragraphe 2, de la directive 2013/36/UE⁷ ;
- 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 efficace⁸ ;

⁷ Orientations de l'ABE sur les politiques de rémunération saines

⁸ Voir également les orientations communes de l'ESMA et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés.

- h. une procédure de sélection et d'évaluation de l'aptitude pour les titulaires de postes clés⁹ ;
 - 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, ainsi que les lignes hiérarchiques entre 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 de l'établissement en matière de prise de risque ;
 - k. une culture et des valeurs d'entreprise conformes à la section 10, qui encouragent 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 des contrôles financiers et opérationnels et la vérification de la conformité à la réglementation et aux normes pertinentes.
23. Lorsqu'ils fixent, approuvent et supervisent la mise en œuvre des aspects énumérés au point 22, l'organe de direction devrait viser à garantir un modèle d'entreprise et des dispositifs de gouvernance, y compris un cadre de gestion des risques, qui tiennent compte de tous les risques. Lorsqu'ils tiennent compte de tous les risques auxquels ils sont exposés, les établissements devraient tenir compte de tous les facteurs de risque pertinents, y compris des risques environnementaux, sociaux et de gouvernance. Les établissements devraient tenir compte du fait que ces derniers peuvent influencer leurs risques prudentiels, y compris leurs risques de crédit (par exemple en raison de facteurs de risque liés à la transition vers une économie durable ou à des événements externes physiques liés au climat, qui peuvent affecter les débiteurs, le marché ou la liquidité), leurs risques opérationnels et leurs risques en matière de réputation (par exemple en raison de facteurs de risque sociaux et de gouvernance, notamment dans le contexte des dispositifs d'externalisation)¹⁰. Ces risques

⁹ Voir également les orientations communes de l'ESMA et de l'ABE sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés.

¹⁰ Voir le rapport de l'ABE sur la gestion et la supervision des risques ESG, publié en vertu de l'article 98, paragraphe 8, de la directive sur les exigences de fonds propres, pour une description de l'interprétation que l'ABE fait des risques ESG et des canaux de transmission, ainsi que des recommandations relatives aux dispositifs, processus, mécanismes et stratégies que les établissements doivent mettre en œuvre pour détecter, évaluer et gérer les risques ESG.

incluent par exemple les risques juridiques dans le domaine du droit des contrats ou du travail, les risques liés aux potentielles violations des droits de l'homme et d'autres facteurs de risque ESG pouvant affecter le pays dans lequel le fournisseur de services est implanté, ainsi que la capacité de ce dernier à fournir les niveaux de service convenus.

24. L'organe de direction doit superviser le processus de publication d'informations et de communication avec les parties prenantes 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 prises 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 surveiller, 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 22 et 23. 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 de façon plus détaillée 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 prendre 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. Pour exercer son jugement et prendre ses décisions, l'organe de direction dans sa fonction exécutive devrait remettre en cause de manière constructive et examiner d'un œil critique les propositions, les explications et les informations reçues. L'organe de direction dans sa fonction exécutive devrait rendre compte globalement 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

conjoncturel dans lequel opère l'établissement, la liquidité et l'assise financière saine ainsi que l'évaluation de ses expositions aux risques d'importance significative.

31. Sans préjudice des dispositions nationales transposant la directive (UE) 2015/849, l'organe de direction devrait identifier l'un de ses membres conformément aux exigences de l'article 46, paragraphe 4, de ladite directive (directive sur la lutte contre le blanchiment de capitaux) en tant que responsable de la mise en œuvre des lois, réglementations et dispositions administratives nécessaires pour satisfaire à ladite directive, y compris des politiques et procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme correspondantes au sein de l'établissement et au niveau de l'organe de direction¹¹.

3 Fonction de surveillance de l'organe de direction

32. 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.
33. Sans préjudice du droit national, l'organe de direction dans sa fonction de surveillance devrait inclure des membres indépendants, comme prévu à la section 9.3 des orientations communes de l'ESMA 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.
34. Sans préjudice des responsabilités attribuées au titre du droit des sociétés national 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 cause 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 des rémunérations et du comité des nominations, si 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, de la stratégie en matière de risque, de l'appétit pour

¹¹L'organe de direction, en sa qualité d'organe collégial, reste collectivement responsable.

le risque et du cadre de gestion des risques de l'établissement, ainsi que d'autres politiques (par exemple la politique de rémunération) et le cadre de publication d'informations ;

- f. vérifier 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 d'un code et 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, si ces comités sont instaurés.

4 Rôle du président de l'organe de direction

- 35. Le président de l'organe de direction devrait diriger l'organe de direction, contribuer à un flux d'information efficace au sein de l'organe de direction et entre l'organe de direction et ses comités, s'ils ont été instaurés, et devrait assumer la responsabilité de son fonctionnement efficace global.
- 36. 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.
- 37. 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 du conseil d'administration éminent ou un membre indépendant supérieur du conseil d'administration 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.

38. 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 prises de manière judicieuse et éclairée et que les documents et les informations sont reçus dans un délai suffisant avant les réunions.
39. 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 Instauration des comités

40. Conformément à l'article 109, paragraphe 1, de la directive 2013/36/UE, lu conjointement avec l'article 76, paragraphe 3, l'article 88, paragraphe 2 et l'article 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 nomination¹² et de rémunération¹³ qui conseillent l'organe de direction dans sa fonction de surveillance et préparent les décisions que ledit organe doit prendre. 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.
41. Si 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.
42. Les établissements peuvent, en tenant compte des critères énoncés au titre I des présentes orientations, instaurer d'autres comités (par exemple des comités de lutte contre le blanchiment de capitaux et le financement du terrorisme, de déontologie, de conduite et de vérification de la conformité).

¹² Voir également les orientations communes de l'ESMA 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 En ce qui concerne le comité des rémunérations, voir les orientations de l'ABE sur les pratiques de rémunération saines.

43. Les établissements devraient garantir une répartition et une distribution claires des attributions et des tâches entre les comités spécialisés de l'organe de direction.
44. Chaque comité devrait recevoir un mandat écrit de la part de l'organe de direction dans sa fonction de surveillance, précisant la portée de ses responsabilités. Il devrait également établir des procédures de travail appropriées.
45. 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 comités¹⁴

46. 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.
47. Les membres indépendants¹⁵ de l'organe de direction dans sa fonction de surveillance devraient participer activement aux comités.
48. Lorsque des comités doivent être instaurés conformément à la directive 2013/36/UE ou au droit national, ils devraient être composés d'au moins trois membres.
49. Les établissements 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.
50. Les établissements devraient envisager la rotation occasionnelle des présidents et des membres des comités, en tenant compte de l'expérience, des connaissances et des compétences spécifiques requises à titre individuel ou collectif pour ces comités.
51. Le comité des risques et le comité des nominations 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/CE¹⁶. Le comité des rémunérations

¹⁴ La présente section devrait être lue conjointement avec les orientations communes de l'ESMA 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.

¹⁵ Au sens de la section 9.3 des orientations communes de l'ESMA 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.

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.

devrait être composé conformément à la section 2.4.1 des orientations de l'ABE sur les politiques de rémunération saines¹⁷.

52. Dans les EISm et les autres EIS, le comité des nominations 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 le droit national, le comité des nominations devrait inclure un nombre suffisant de membres indépendants. Ces établissements peuvent également envisager comme bonne pratique de nommer à la présidence du comité des nominations un membre indépendant.
53. Les membres du comité des nominations devraient disposer, à titre individuel et collectif, de connaissances, de compétences et d'une expertise appropriées concernant le processus de sélection et les exigences d'aptitudes en matière d'adéquation visées dans la directive 2013/36/UE.
54. 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 le droit national, 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.
55. Les membres du comité des risques devraient disposer, à titre individuel et collectif, des connaissances, des compétences et de l'expertise appropriées concernant les pratiques de gestion et de contrôle des risques.

5.3 Procédures des comités

56. Les comités devraient faire rapport régulièrement à l'organe de direction dans sa fonction de surveillance.
57. Les comités devraient interagir entre eux, en tant que de besoin. Sans préjudice du point 49, 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.
58. Les membres des comités devraient participer à des discussions ouvertes et analytiques, au cours desquelles les différences d'opinion sont discutées de manière constructive.
59. Les comités devraient documenter l'ordre du jour de leurs réunions, ainsi que leurs principaux résultats et conclusions.

¹⁷ 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 (EBA/GL/2015/22).

60. Le comité des risques et le comité des nominations devraient, à tout le moins:

- a. avoir accès à toutes les informations et données pertinentes dont ils ont besoin pour accomplir leur rôle, y compris celles fournies par les fonctions d'entreprise et de contrôle pertinentes (par exemple les services juridique, des finances, des ressources humaines, informatique, de l'audit interne, de la gestion des risques et de la vérification de la conformité, y compris des informations sur la conformité aux règles de lutte contre le blanchiment de capitaux et le financement du terrorisme et des informations agrégées sur les déclarations de transactions suspectes et les facteurs de risque liés au blanchiment de capitaux et au financement du terrorisme);
- b. recevoir des rapports réguliers, des informations ad hoc, des communications et des opinions de la part des responsables des fonctions de contrôle interne concernant le profil de risque actuel de l'établissement, sa culture du risque et ses limites de risque, ainsi que toute violation significative ¹⁸ pouvant être survenue, accompagnés d'informations détaillées et de recommandations sur les mesures correctives prises, à prendre ou proposées en vue de leur examen, ainsi que réexaminer périodiquement et déterminer le contenu, le format et la fréquence des informations sur les risques devant leur être communiquées; et
- c. en tant que de besoin, garantir la participation adéquate des fonctions de contrôle interne et autres fonctions pertinentes (ressources humaines, juridique, finances) dans leur domaine d'expertise respectif et/ou solliciter les conseils d'experts externes.

5.4 Rôle du comité des risques

61. S'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 la surveillance 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 d'entreprise et aux valeurs 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 la liquidité, ainsi que des autres risques pertinents tels que le risque de marché, le risque de crédit, le risque opérationnel (y compris les risques

¹⁸ S'agissant des violations graves des règles de lutte contre le blanchiment de capitaux et le financement du terrorisme. Voir également les orientations devant être émises en vertu de l'article 117, paragraphe 6, de la directive 2013/36/UE, qui précisent les modalités de la coopération et de l'échange d'informations entre les autorités visées au paragraphe 5 dudit article, en particulier en ce qui concerne les groupes transfrontières et dans le contexte de la détection des violations graves des règles de lutte contre le blanchiment de capitaux.

juridique et informatique) et le risque de réputation, afin d'évaluer leur adéquation par rapport à la stratégie en matière de risque et à l'appétit pour le risque approuvés ;

- d. fournir à l'organe de direction dans sa fonction de surveillance des recommandations sur les ajustements 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 de l'aide ;
 - 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 de l'établissement en matière de risque¹⁹. 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 prises.
62. 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 des rémunérations) et communiquer régulièrement avec les fonctions de contrôle interne de l'établissement, notamment avec la fonction de gestion des risques.
63. S'il est instauré, le comité des risques doit, sans préjudice des tâches du comité des rémunérations, examiner si les incitations proposées par les politiques et pratiques de rémunération tiennent compte du risque, du capital, 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

64. Conformément à la directive 2006/43/CE²⁰, lorsqu'il est instauré, le comité d'audit devrait, entre autres :

¹⁹ Voir également les 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>.

²⁰ 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

- a. surveiller 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 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. surveiller le processus d'élaboration de l'information financière et communiquer des recommandations visant à garantir son intégrité ;
- d. examiner et surveiller 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° 537/2014²¹, et notamment le caractère approprié de la prestation de services autres que d'audit à l'établissement contrôlé conformément à l'article 5 dudit règlement ;
- e. surveiller 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 externes ou des cabinets d'audit et recommander l'approbation par l'organe compétent de l'établissement de leur nomination (conformément à l'article 16 du règlement (UE) n° 537/2014, sauf lorsque l'article 16, paragraphe 8, dudit règlement est appliqué), 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, ainsi que 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

65. 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

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.

²¹ 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).

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.

66. 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.
67. Les établissements 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 commun²².

Titre III – Cadre de gouvernance

6 Cadre organisationnel et structure

6.1 Cadre organisationnel

68. 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 nécessaires pour exercer leur rôle de manière efficace. Les rapports hiérarchiques et la répartition des responsabilités au sein de l'établissement, notamment entre titulaires de postes clés, devraient être clairs, bien définis, cohérents, exécutoires et dûment documentés. La documentation devrait être dûment actualisée.
69. 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.
70. L'organe de direction devrait déterminer si des modifications significatives de la structure du groupe (par exemple la création de nouvelles filiales, des fusions et acquisitions, la vente ou la liquidation de parties du groupe ou des événements externes) ont une incidence sur la solidité du cadre organisationnel de l'établissement et, dans l'affirmative, laquelle. Si des

²² Voir également les orientations communes de l'ESMA 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.

faiblesses sont détectées, l'organe de direction devrait procéder sans délai à tout ajustement nécessaire.

6.2 Connaissance de sa propre structure

71. 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 la stratégie économique, la stratégie en matière de risque et l'appétit pour le risque qui ont été approuvés et qui sont couverts par son cadre de gestion des risques.
72. 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.
73. 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.
74. 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.
75. 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 pour appréhender clairement les objectifs généraux, les stratégies et le profil de risque du groupe, ainsi que la façon 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

76. Les établissements devraient éviter la mise en place de structures complexes et potentiellement non transparentes. Les établissements devraient tenir compte, dans leurs prises 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, au financement du terrorisme ou à d'autres délits financiers, ainsi que des contrôles et du cadre juridique respectifs en place²³. 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 et sur la lutte contre le blanchiment de capitaux et le financement du terrorisme²⁴ ;
- 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 l'éventuelle création d'une structure donne lieu à des préoccupations ;

²³ Pour des informations plus détaillées sur l'évaluation du risque-pays et du risque inhérent aux produits et clients individuels, les établissements devraient également se référer aux orientations communes sur les facteurs de risque en matière de blanchiment de capitaux et de financement du terrorisme (EBA GL JC/2017/37), actuellement en cours de réexamen.

²⁴ Voir également: <https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rti-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries>

- 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.
77. En tout état de cause, les établissements ne devraient pas créer de structures opaques ou inutilement complexes n'ayant pas de justification économique claire ou d'objectif juridique, ni de structures dont l'on pourrait penser qu'elles ont été créées à des fins liées à des délits financiers.
78. Lorsqu'il crée de telles structures, l'organe de direction devrait les comprendre, ainsi que leur objectif et les risques particuliers qui y sont associés, et veiller à ce que les fonctions de contrôle interne soient dûment associées à 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 détectés, 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.
79. Les établissements devraient documenter leurs décisions et être en mesure de les justifier auprès des autorités compétentes.
80. L'organe de direction devrait s'assurer que des mesures appropriées sont prises pour prévenir ou atténuer les risques liés aux activités au sein des ces structures. Il s'agit notamment de veiller à ce que :
- a. l'établissement dispose de politiques et procédures adéquates et de processus documentés (par exemple des limites applicables, des 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, ainsi qu'à l'autorité compétente qui a octroyé l'agrément ;
 - c. l'établissement évalue périodiquement s'il y a lieu de maintenir de telles structures.

81. Ces structures et activités, y compris leur conformité à la réglementation et aux 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.
82. 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

83. 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, y compris dans celles qui sont établies dans des pays tiers, centres financiers extraterritoriaux compris, afin d'assurer un dispositif solide de gouvernance sur base consolidée et sous-consolidée. S'agissant des exigences relatives à la rémunération, quelques exceptions s'appliquent, conformément à l'article 109, paragraphes 4 et 5²⁵. 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.
84. L'organe de direction d'une filiale relevant de la directive 2013/36/UE devrait adopter et mettre en œuvre au niveau individuel des politiques de gouvernance pour l'ensemble du groupe, établies au niveau consolidé ou sous-consolidé, d'une manière conforme à l'ensemble des exigences particulières au titre du droit national et de l'UE.
85. Aux niveaux consolidé et sous-consolidé, l'établissement consolidant devrait garantir le respect des politiques de gouvernance de l'ensemble du groupe et du cadre de contrôle interne visé au titre V 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

²⁵ Voir également les orientations de l'ABE sur les politiques de rémunération saines

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.

86. 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.
87. Les entreprises mères et leurs filiales devraient veiller à ce que les établissements et les entités au sein du groupe respectent toutes les exigences réglementaires spécifiques à toute juridiction pertinente.
88. 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.
89. Les exigences en matière de gouvernance énoncées dans la directive 2013/36/UE et les dispositions des 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 à l'échelle du groupe de l'établissement mère 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, ni aux précisions supplémentaires des présentes orientations.
90. 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'externalisation²⁶

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

²⁶ Voir également: orientations de l'ABE relatives à l'externalisation, disponibles à l'adresse <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements>

92. 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 juridiques et informatiques, 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.
93. 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. La politique devrait également couvrir l'externalisation intragroupe (à savoir les services fournis par une entité juridique séparée au sein du groupe d'un établissement) et tenir compte de toute circonstance particulière du groupe.

Titre IV – Culture du risque et bonne conduite commerciale

9 Culture du risque

94. Une culture du risque solide, diligente et cohérente devrait être un élément clé de la gestion efficace des risques des établissements et devrait permettre aux établissements de prendre 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 des 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 nécessairement s'y limiter, une culture du risque solide devrait inclure ce qui suit :

- a. Exemple montré par 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 de l'établissement. La direction des établissements, y compris les titulaires de postes clés, devrait contribuer à la communication interne, auprès du personnel, des principales valeurs et attentes. Le personnel devrait agir dans le respect de toutes les lois et réglementations applicables et communiquer rapidement aux niveaux hiérarchiques supérieurs les cas de non-conformité observés au sein ou à l'extérieur de l'établissement (par exemple à l'autorité compétente par une procédure de dénonciation des dysfonctionnements). L'organe de direction devrait promouvoir, surveiller 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, selon les besoins.
- b. Obligation de rendre compte : les membres du personnel concernés, 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 conscients qu'ils devront assumer la responsabilité de leurs actes dans le cadre du comportement de l'établissement en matière de prise de risque.
- 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, facilitent 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'harmonisation du comportement de prise de risque avec le profil de risque de l'établissement et ses intérêts à long terme²⁷.

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

²⁷ 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 (EBA/GL/2015/22), disponibles à l'adresse <https://www.eba.europa.eu/regulation-and-policy/remuneration>.

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 établissements devraient veiller à ce que leur personnel ne subisse aucune discrimination fondée sur le sexe, la race, la couleur de peau, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou autres, l'appartenance à une minorité nationale, la fortune, la naissance, le handicap, l'âge ou l'orientation sexuelle.
101. Les politiques de l'établissement devraient être neutres du point de vue du genre. Cela concerne notamment, mais pas uniquement, la rémunération, les politiques de recrutement, le développement professionnel, les plans de succession, l'accès à la formation et la capacité à postuler à des postes en interne. Les établissements devraient garantir l'égalité des chances²⁸ à tous les membres du personnel, quel que soit leur genre, y compris dans le cadre de leurs perspectives professionnelles, et devraient chercher à améliorer la représentation du sexe sous-représenté aux postes de l'organe de direction, ainsi que parmi les membres du personnel exerçant des fonctions de direction, selon la définition fournie dans le règlement délégué de la Commission (normes techniques de réglementation sur le personnel identifié)²⁹. Les établissements devraient surveiller séparément l'évolution de l'écart de rémunération entre les hommes et les femmes parmi les membres du personnel identifié (à l'exception des membres de l'organe de direction), les membres de l'organe de direction dans sa fonction exécutive, les membres de l'organe de direction dans sa fonction de surveillance et les autres membres du personnel. Les établissements devraient instaurer des politiques facilitant la réintégration des membres du personnel après un congé de maternité, de paternité ou parental.
102. Les normes mises en œuvre devraient viser à renforcer davantage les solides dispositifs de gouvernance de l'établissement et 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 en raison d'amendes, de frais judiciaires, de restrictions imposées par les autorités compétentes, d'autres sanctions financières et pénales, ainsi que la perte de valeur de la marque et la détérioration de la confiance des consommateurs.
103. 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 :

²⁸ Voir également la directive 2006/54/CE du Parlement européen et du Conseil du 5 juillet 2006 relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail

²⁹ Voir également les orientations de l'ABE sur les politiques de rémunération neutres du point de vue du genre

- a. rappeler au personnel que toutes les activités de l'établissement devraient être menées conformément au droit 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 financières, aux mauvaises conduites financières et à la criminalité économique ou financière, incluant sans s'y limiter la fraude, le blanchiment de capitaux, le financement du terrorisme, les pratiques anti-trust, les sanctions financières, la corruption active et passive, la manipulation de marché, la vente abusive, d'autres violations de la réglementation en matière de protection des consommateurs et les délits fiscaux, que ces actes soient commis directement ou indirectement, y compris par le biais de pratiques d'arbitrage de dividendes illicites ou interdites ;
 - 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.
104. Les établissements devraient vérifier le respect de ces normes et veiller à la sensibilisation du personnel, par exemple en offrant des formations. Les établissements devraient définir la fonction chargée de contrôler la conformité au code de conduite, ou à des documents similaires, et d'évaluer les violations du code de conduite ou autres documents, 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

105. 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 détecter, 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 parties prenantes externes.

106. 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.
107. Les mesures prises par les établissements pour 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.

12 Politique en matière de conflits d'intérêts pour le personnel³⁰

108. 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 visant à détecter, 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 des membres de l'organe de direction, qui pourraient avoir une incidence défavorable sur l'exercice de leurs attributions et responsabilités. Un établissement consolidant devrait tenir compte des intérêts dans le cadre d'une politique en matière de conflits d'intérêts à l'échelle du groupe sur base consolidée ou sous-consolidée.
109. La politique devrait viser à détecter 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 définir puis mettre en œuvre des mesures d'atténuation appropriées.
110. En ce qui concerne les conflits d'intérêts susceptibles de résulter de relations antérieures, les établissements devraient fixer une période appropriée durant 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.
111. La politique devrait couvrir à tout le moins les situations ou relations suivantes dans lesquelles des conflits d'intérêts peuvent survenir :

³⁰ La présente section devrait être lue conjointement avec les orientations communes de l'ESMA 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 accordés 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 des membres du personnel de l'établissement ou d'entités incluses dans le périmètre de consolidation prudentielle (par exemple les relations familiales) ;
 - d. autre emploi et emploi antérieur dans le passé récent (par exemple cinq ans) ;
 - e. relations personnelles ou professionnelles avec des parties prenantes externes (par exemple une association avec des fournisseurs, des consultants ou d'autres prestataires de services d'importance significative) ; et
 - f. influence politique ou relations politiques.
112. 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 concerné est considéré comme présentant un conflit d'intérêts, dès lors qu'il demeure en-deçà d'un seuil de minimis approprié.
113. La politique devrait énoncer les procédures de déclaration et de communication à la fonction responsable au titre de la politique. Les membres du personnel concernés devraient être tenus de déclarer sans délai à l'établissement toute situation susceptible de créer un conflit d'intérêts ou ayant déjà causé un conflit d'intérêts.
114. La politique devrait opérer une distinction entre les conflits d'intérêts qui persistent et qui doivent être gérés de manière permanente et les conflits d'intérêts qui surviennent de manière inattendue dans le cadre d'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 ponctuelle. Dans tous les cas, l'intérêt de l'établissement devrait être l'élément déterminant pour la prise de décisions.
115. La politique devrait énoncer les procédures, les mesures, les éléments de documentation et les responsabilités concernant la détection et la prévention de conflits d'intérêts en vue d'évaluer leur importance et de prendre des mesures d'atténuation. Ces procédures, éléments, responsabilités et mesures devraient inclure ce qui suit:

- a. confier les activités ou 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 à remplir correctement leurs obligations envers l'établissement pourraient être compromises de toute autre manière ;
 - d. empêcher les membres de l'organe de direction de détenir des directorats dans des établissements concurrents, à moins qu'il s'agisse d'établissements faisant partie du même système de protection institutionnel, tel que 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, tels que visés à l'article 10 du règlement (UE) n° 575/2013, ou d'établissements entrant dans le périmètre de consolidation prudentielle.
116. 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 direction³¹.
117. Pour atténuer les conflits d'intérêts détectés parmi les membres de l'organe de direction, les établissements devraient documenter les mesures prises, y compris les arguments démontrant l'efficacité de ces mesures, afin de garantir des prises de décisions objectives.
118. 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 prise, notamment si le conflit d'intérêts et les risques y afférents ont été acceptés, et, si le conflit d'intérêts a été accepté, la manière dont il a été atténué ou résolu de manière satisfaisante.
119. 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.

³¹ Voir également les orientations communes de l'ESMA 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.

12.1 Politique en matière de conflits d'intérêts dans le contexte des prêts et autres transactions effectuées avec les membres de l'organe de direction et leurs parties liées

120. Dans le cadre de leur politique en matière de conflits d'intérêts pour le personnel (section 12) et de la gestion des conflits d'intérêts des membres de l'organe de direction, comme indiqué au point 117, l'organe de direction devrait établir un cadre permettant de détecter et de gérer les conflits d'intérêts dans le contexte de l'octroi de prêts et de l'exécution d'autres transactions avec les membres de l'organe de direction et leurs parties liées (par exemple des opérations d'affacturage, de crédit-bail, transactions immobilières, etc.)
121. Sans préjudice des dispositions nationales transposant la directive 2013/36/UE³², les établissements peuvent envisager d'ajouter des catégories supplémentaires de parties liées auxquelles ils appliquent, dans sa totalité ou en partie, le cadre des conflits d'intérêts s'agissant des prêts et autres transactions.
122. Le cadre des conflits d'intérêts devrait permettre de garantir que les décisions relatives à l'octroi de prêts et à l'exécution d'autres transactions avec les membres de l'organe de direction et leurs parties liées sont prises de façon objective, sans influence injustifiée des conflits d'intérêts, et sont en principe prises dans des conditions normales de concurrence.
123. L'organe de direction devrait instaurer les processus de prise de décision applicables à l'octroi de prêts et à l'exécution d'autres transactions avec les membres de l'organe de direction et leurs parties liées. Ce cadre peut prévoir une différenciation entre, d'une part, les opérations commerciales ordinaires³³ conclues dans le cadre ordinaire d'activité et selon des conditions normales de marché et, d'autre part, les prêts et transactions impliquant les membres du personnel, qui sont effectués selon des conditions proposées à tous les membres du personnel. De plus, le cadre des conflits d'intérêts et le processus de prise de décision peuvent établir une différence entre les prêts et autres transactions ayant une importance significative ou non, entre différents types de prêts et autres transactions et entre différents niveaux de conflit d'intérêts potentiel ou avéré qu'ils peuvent engendrer.
124. Dans le contexte du cadre des conflits d'intérêts, l'organe de direction devrait définir des seuils appropriés (par exemple par type de produit ou en fonction des conditions), au-dessus desquels les prêts et autres transactions effectués avec des membres de l'organe de direction ou leurs parties liées nécessitent toujours l'approbation de l'organe de direction. Les décisions relatives aux prêts et autres transactions ayant une importance significative, qui sont effectués avec les membres de l'organe de direction non pas selon des conditions normales

³² Voir également le principe fondamental de Bâle n° 20

³³ Les opérations commerciales incluent les prêts et autres transactions (par exemple des opérations de crédit-bail, des opérations d'affacturage, des services liés aux introductions en bourse, des fusions et acquisitions et des opérations d'achat ou de vente de biens immobiliers).

de marché mais selon des conditions proposées à tous les membres du personnel, devraient toujours être prises par l'organe de direction.

125. Le membre de l'organe de direction bénéficiant d'un tel prêt ou d'une telle transaction ayant une importance significative, ou le membre lié à la contrepartie, ne devrait pas participer à la prise de décision.
126. Avant de prendre une décision relative à un prêt accordé ou à une autre transaction effectuée avec un membre de l'organe de direction ou ses parties liées, les établissements devraient évaluer les risques auxquels ils pourraient s'exposer en raison du prêt ou de la transaction.
127. Si des prêts sont accordés en tant que ligne de crédit (par exemple un découvert bancaire), la décision initiale et toute modification afférente devraient être documentées. Toute utilisation de telles facilités de crédit, dans les limites convenues, ne devrait pas être considérée comme une nouvelle décision relative à un prêt accordé à un membre de l'organe de direction ou à l'une de ses parties liées. Si une modification apportée à une ligne de crédit a une importance significative selon la politique de l'établissement, une nouvelle évaluation devrait être effectuée et une nouvelle décision devrait être prise.
128. Afin de garantir la conformité à leurs politiques en matière de conflits d'intérêts, les établissements devraient veiller, d'une part, à ce que toutes les procédures de contrôle interne pertinentes soient entièrement appliquées aux prêts et autres transactions avec des membres de l'organe de direction ou leurs parties liées et, d'autre part, à ce qu'un cadre de supervision approprié soit mis en place au niveau de l'organe de direction dans sa fonction de surveillance.

12.2 Documentation des prêts accordés aux membres de l'organe de direction et à leurs parties liées, et informations complémentaires

129. Aux fins de l'article 88, paragraphe 1, de la directive 2013/36/UE, les établissements devraient documenter les données relatives aux prêts³⁴ accordés aux membres de l'organe de direction et à leurs parties liées, en incluant au moins les éléments suivants:
 - a. le nom du débiteur et son statut (membre de l'organe de direction ou partie liée) et, s'agissant des prêts octroyés à une partie liée, le membre de l'organe de direction à qui cette partie est liée et la nature de sa relation avec la partie liée ;
 - b. le type/la nature du prêt et son montant ;
 - c. les conditions générales applicables au prêt ;

³⁴ Voir également les orientations de l'ABE sur l'octroi et le suivi des prêts, disponibles à l'adresse: <https://eba.europa.eu/regulation-and-policy/credit-risk/guidelines-on-loan-origination-and-monitoring>

- d. la date d’approbation du prêt ;
 - e. le nom de la personne ou de l’organe décidant d’approuver le prêt, ainsi que la composition de l’organe, et les conditions applicables ;
 - f. le fait que le prêt ait ou non été octroyé selon les conditions du marché ; et
 - g. le fait que le prêt ait ou non été octroyé selon des conditions proposées à tous les membres du personnel.
130. Les établissements devraient veiller à ce que la documentation de tous les prêts octroyés aux membres de l’organe de direction et à leurs parties liées soit complète et à jour. Ils devraient également s’assurer de pouvoir fournir aux autorités compétentes la documentation complète, dans un format approprié, sur demande et sans retard injustifié.
131. Dans le cadre d’un prêt octroyé à un membre de l’organe de direction ou à l’une de ses parties liées dont le montant est supérieur à 200 000 euros, les établissements devraient pouvoir fournir à l’autorité compétente, sur demande, les informations complémentaires suivantes :
- a. le pourcentage du prêt et le pourcentage de la somme de tous les encours de crédit concernant le même débiteur, par rapport aux éléments suivants :
 - i. la somme de ses fonds propres de base et de ses fonds propres complémentaires, et
 - ii. les fonds propres de base de catégorie 1 de l’établissement ;
 - b. le fait que le prêt fasse partie ou non d’un grand risque³⁵ ; et
 - c. le poids relatif de la somme agrégée de tous les encours de crédit concernant le même débiteur, calculé en tant que pourcentage en divisant l’encours total par le montant total de tous les encours de crédit concernant les membres de l’organe de direction et leurs parties liées.

13 Procédures d’alerte interne

132. Les établissements devraient mettre en place et maintenir des politiques et procédures appropriées en matière d’alerte interne pour que le personnel puisse signaler des violations potentielles ou avérées des exigences réglementaires ou internes, incluant sans s’y limiter 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, mais il devrait cependant avoir un niveau de certitude suffisant constituant une raison suffisante pour ouvrir une enquête. Les établissements devraient également mettre en œuvre des processus et procédures

³⁵ Voir également la partie IV du règlement (UE) n° 575/2013, notamment l’article 392.

appropriés leur permettant de respecter les obligations qui leur incombent en vertu de la transposition, dans le droit national, de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

133. Afin d'éviter les conflits d'intérêts, il devrait être possible pour le personnel de signaler les 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 présumée responsable de la violation, conformément au règlement (UE) 2016/679 (RGPD)³⁶.
134. Les procédures d'alerte devraient être mises à la disposition de l'ensemble du personnel de l'établissement.
135. 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.
136. Les établissements devraient garantir que la personne signalant la violation est dûment protégée contre toute incidence défavorable, par exemple des représailles, de la discrimination ou d'autres types de traitement injuste. L'établissement devrait garantir qu'aucune personne sous son contrôle ne se rende coupable de victimisation envers une personne ayant signalé une violation et devrait prendre des mesures appropriées contre les responsables d'une telle victimisation.
137. Les établissements devraient également protéger les personnes dénoncées contre toute conséquence défavorable, si l'enquête ne fait apparaître aucune preuve justifiant de prendre des mesures contre ces personnes. Si des mesures sont prises, 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 prise.
138. Plus précisément, les procédures d'alerte interne devraient :
 - a. être documentées (par exemple des manuels pour le personnel) ;

³⁶ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

- 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 au règlement (UE) 2016/679, 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 la victimisation après avoir divulgué des violations à signaler ;
- d. garantir que les violations potentielles ou avérées signalées sont évaluées et communiquées aux niveaux hiérarchiques supérieurs, y compris, le cas échéant, à l'autorité compétente ou aux services répressifs pertinents ;
- 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 de toute enquête concernant une violation signalée ; et
- g. garantir la conservation appropriée des dossiers.

14 Signaler des violations aux autorités compétentes

139. Les autorités compétentes devraient mettre en place des mécanismes efficaces et fiables permettant au personnel des établissements de signaler aux autorités compétentes les violations potentielles ou avérées d'exigences réglementaires, incluant sans s'y limiter 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 dédié(e) 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 présumée responsable de la violation, conformément au règlement (UE) 2016/679 (RGPD) ; et
- d. des procédures claires comme prévu à la section 13.

140. 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

141. 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 dans l'exercice de 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.
142. Le cadre de contrôle interne des établissements devrait être adapté sur une base individuelle à la particularité de leurs activités, leur complexité et les risques associés, en tenant compte du contexte du groupe. Les établissements devraient 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, ainsi que la fonction de vérification de la conformité aux règles de lutte contre le blanchiment de capitaux et le financement du terrorisme si celle-ci est une fonction de contrôle distincte, 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.
143. Les établissements devraient mettre en œuvre des processus et procédures appropriés leur permettant de respecter les obligations qui leur incombent en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Les établissements devraient évaluer leur exposition au risque d'être utilisés à des fins de blanchiment de capitaux ou de financement du terrorisme et, si nécessaire, prendre des mesures d'atténuation visant à réduire ce risque, ainsi que les risques opérationnel et de réputation associés. Les établissements devraient prendre des mesures permettant de garantir que les membres de leur personnel connaissent ces risques de blanchiment de capitaux et de financement du terrorisme, ainsi que l'impact que ces pratiques ont sur l'établissement concerné et l'intégrité du système financier.
144. 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.
145. 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

146. L'organe de direction devrait être responsable de la mise en place et de la surveillance 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 unités internes, y compris les fonctions de contrôle interne (telles que la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction de vérification de la conformité aux règles de lutte contre le blanchiment de capitaux et le financement du terrorisme si celle-ci est une fonction de contrôle distincte et la fonction 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.
147. L'établissement devrait être doté d'un processus de prise de décisions clair, transparent et documenté et prévoir une répartition claire des responsabilités et de l'autorité au sein de son cadre de contrôle interne, y compris ses lignes d'activité, unités internes et fonctions de contrôle interne.
148. Les établissements devraient communiquer ces politiques, mécanismes et procédures à l'ensemble du personnel et chaque fois que des modifications significatives y sont apportées.
149. 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.

150. Les fonctions de contrôle interne devraient vérifier que les politiques, mécanismes et procédures énoncés dans le cadre de contrôle interne sont correctement mis en œuvre dans leurs domaines de compétence respectifs.
151. 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 toute nouvelle lacune importante détectée, les risques pertinents, une analyse d'impact, des recommandations et des mesures correctives à prendre. L'organe de direction devrait assurer le suivi des constats des fonctions de contrôle interne en temps utile et de manière efficace et exiger des mesures correctives adéquates. Une procédure formelle de suivi des constats et des mesures correctives prises devrait être mise en place.

17 Cadre de gestion des risques

152. 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 de prendre des décisions éclairées sur la prise de risque. Le cadre de gestion des risques devrait inclure les risques de bilan et 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 inclus dans le cadre de gestion des risques en tenant dûment compte des risques tant financiers que non financiers, y compris le risque de crédit, le risque de marché, le risque de liquidité, le risque de concentration, le risque opérationnel, le risque informatique, le risque de réputation, le risque juridique, le risque lié à la conduite, le risque lié à la conformité aux règles de lutte contre le blanchiment de capitaux, le financement du terrorisme et d'autres crimes financiers, le risque lié aux critères ESG et le risque stratégique.
153. Le cadre de gestion des risques de l'établissement devrait inclure des politiques, des procédures, des limites de risque et des contrôles des risques lui permettant de détecter, de mesurer ou d'évaluer, de surveiller, 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.
154. Le cadre de gestion des risques de l'établissement devrait fournir des recommandations spécifiques sur la mise en œuvre de ses stratégies. Ces recommandations devraient, le cas échéant, fixer et maintenir des limites internes conformes à l'appétit pour le risque de l'établissement et proportionnées à 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.

155. Le cadre de gestion des risques devrait faire l'objet d'un examen interne indépendant, réalisé par exemple par la fonction d'audit interne, et être régulièrement réévalué par rapport à l'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, le profil de risque ou la structure opérationnelle, l'expansion géographique, les fusions et acquisitions et le lancement de nouveaux produits ou la mise en œuvre de nouvelles branches d'activité.
156. S'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'agrégier les expositions aux risques dans toutes les lignes d'activité et contribuer à détecter 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 de l'établissement à prendre des risques. 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.
157. 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 découler d'une faiblesse du modèle (par exemple l'exclusion de certains risques pertinents) plutôt que d'une stratégie supérieure ou de 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 inclure une approche qualitative (y compris un jugement d'expert et une analyse critique). Il convient de prendre en considération de manière explicite les tendances et les données pertinentes du contexte macroéconomique afin de déterminer leur incidence potentielle sur les expositions et les portefeuilles.
158. 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.

159. 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).
160. 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.
161. Des mécanismes de déclaration réguliers et transparents devraient être établis afin que l'organe de direction, son comité des risques (s'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, la surveillance et la gestion des risques. Le cadre de déclaration devrait être bien défini et documenté.
162. Une communication efficace et la connaissance des risques, ainsi que 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 les risques à l'insu de l'établissement. 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 des expositions et des 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 significatifs³⁷

163. 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 (par exemple les processus de changements informatiques) afférents. 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, ainsi qu'avec les limites correspondantes, ou que les révisions nécessaires sont faites.

³⁷ 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>.

164. Les changements significatifs et 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 survenant après la fusion, la mise en place de structures (par exemple nouvelles filiales ou entités ad hoc), les nouveaux produits, les changements apportés aux systèmes ou au cadre ou procédures de gestion des risques et les changements apportés à l'organisation de l'établissement.
165. L'établissement devrait disposer de procédures spécifiques pour évaluer la conformité à 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.
166. 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.
167. La PVNP devrait définir les principales questions à examiner avant qu'une décision ne soit arrêtée. Celles-ci comprennent notamment la conformité à la réglementation, la comptabilité, les modèles tarifaires, l'incidence sur le profil de risque, l'adéquation des fonds propres et la rentabilité, la disponibilité de ressources adéquates pour le front office, le back office et le middle office, ainsi que la disponibilité d'outils internes adéquats et de connaissances techniques suffisantes pour comprendre et contrôler les risques y afférents. De plus, afin de respecter les obligations qui leur incombent en vertu de la directive (UE) 2015/849, les établissements devraient détecter et évaluer les risques de blanchiment de capitaux et de financement du terrorisme associés à un nouveau produit ou une nouvelle pratique commerciale et définir les mesures à prendre pour les atténuer. La décision de lancer une nouvelle activité devrait indiquer 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.
168. 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 dans 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 lignes d'activité, ainsi que 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

169. Les fonctions de contrôle interne devraient inclure 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. Les responsabilités des fonctions de contrôle visent également à assurer la conformité aux exigences en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.
170. Les tâches opérationnelles des fonctions de contrôle interne peuvent être externalisées, en tenant compte des critères de proportionnalité énoncés au titre I, vers l'établissement consolidant ou vers 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.
171. Sans préjudice du droit national transposant la directive (UE) 2015/849, les établissements devraient attribuer la responsabilité de garantir la conformité de l'établissement aux exigences de ladite directive et aux politiques et procédures de l'établissement à un membre du personnel (par exemple le responsable de la conformité). Les établissements peuvent instaurer une fonction de vérification de la conformité distincte en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, en tant que fonction de contrôle indépendante³⁸. La personne responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme devrait pouvoir, si nécessaire, rendre des comptes directement à l'organe de direction dans sa fonction exécutive et dans sa fonction de surveillance.

19.1 Responsables des fonctions de contrôle interne

172. Les responsables des fonctions de contrôle interne devraient être mis en place à un niveau hiérarchique adéquat leur conférant l'autorité et le statut 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 auprès de l'organe de direction et leurs performances devraient être réexaminées par l'organe de direction.

³⁸ Voir également les orientations de l'ABE sur la fonction de vérification de la conformité aux règles de lutte contre le blanchiment de capitaux et le financement du terrorisme (actuellement en cours de développement)

173. Si nécessaire, les responsables de fonctions de contrôle interne devraient pouvoir avoir accès et 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.
174. Les établissements devraient disposer de procédures documentées pour pourvoir le poste de responsable d'une fonction de contrôle interne et pour retirer les responsabilités de cette personne. 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 – ses – fonctions sans l'accord préalable de l'organe de direction dans sa fonction de surveillance. S'agissant des établissements ayant une importance significative, les autorités compétentes devraient être immédiatement informées de l'approbation et des principales raisons de la révocation d'un responsable d'une fonction de contrôle interne.

19.2 Indépendance des fonctions de contrôle interne

175. 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 l'exécution des activités que celles-ci surveillent et contrôlent, et ne devrait pas nuire à leur objectivité de quelque autre manière que ce soit³⁹.

³⁹ 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>.

19.3 Fonctions de contrôle interne communes

176. 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 combinées. La fonction d'audit interne ne devrait pas être combinée avec une autre fonction de contrôle interne.

19.4 Ressources des fonctions de contrôle interne

177. 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.
178. 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

179. 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 visé à la section 17.
180. Si nécessaire, la FGR devrait avoir un accès direct à l'organe de direction dans sa fonction de surveillance et à ses comités, s'ils sont instaurés, y compris notamment le comité des risques.
181. 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 sociétés affiliées pertinentes.
182. Le personnel de la FGR devrait disposer de connaissances, de compétences et d'une expérience suffisantes s'agissant des techniques et procédures de gestion des risques, ainsi que des marchés et des produits, et devrait avoir accès à une formation régulière.
183. 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 de réaliser l'objectif de l'ensemble du personnel de l'établissement responsable de la gestion des risques.
184. La FGR devrait constituer un élément organisation central 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.

185. 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 y avoir une FGR centrale, y compris une FGR de groupe au sein de 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.
186. La FGR devrait fournir des informations, analyses et expertises indépendantes et pertinentes sur les expositions aux risques et formuler des conseils quant aux propositions et décisions en matière de risque prises par les lignes d'activité ou les unités internes. Elle devrait également indiquer à l'organe de direction si ces informations, analyses et expertises sont cohérentes avec la stratégie en matière de risque et l'appétit pour le 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 aux 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

187. 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 sur les 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 des limites de risque spécifiques sont instaurées en fonction de l'appétit pour le risque. La FGR devrait également évaluer la stratégie en matière de risque et l'appétit pour le risque des unités opérationnelles, y compris les objectifs proposés par les unités opérationnelles. Elle devrait également être consultée avant qu'une décision soit prise par l'organe de direction concernant la stratégie en matière de risque et l'appétit pour le risque. Les objectifs devraient être plausibles et cohérents avec la stratégie en matière de risque de l'établissement.
188. 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

189. 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 qu'une décision ne soit prise.
190. La FGR devrait évaluer dans quelle mesure les risques détectés 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 Rôle de la FGR en matière de détection, de mesure, d'évaluation, de gestion, d'atténuation, de suivi et de déclaration des risques

191. La FGR devrait veiller à ce qu'un cadre de gestion des risques approprié soit mis en place et à ce que tous les risques soient détectés, évalués, mesurés, surveillés, gérés et dûment déclarés par les unités de l'établissement concernées.
192. La FGR devrait veiller à ce 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.
193. 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 détectés et dûment évalués.
194. La FGR devrait s'assurer que tous les risques détectés font l'objet d'une surveillance efficace par les unités opérationnelles.
195. 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.
196. La FGR devrait analyser les tendances et déceler les risques nouveaux ou émergents, ainsi que l'accroissement des risques, liés à l'évolution des conditions et des circonstances. Elle devrait également réexaminer régulièrement les résultats en matière de risques avérés par rapport aux estimations antérieures (contrôles a posteriori), afin d'évaluer et d'améliorer la précision et l'efficacité du processus de gestion des risques.

197. 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 les mesures qu'il est proposé de prendre pour atténuer les risques.

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

198. 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, ainsi que 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.
199. La FGR devrait jouer un rôle essentiel pour garantir qu'une décision est prise au niveau approprié à la suite d'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, s'il est instauré, au comité des risques.

20.5 Responsable de la fonction de gestion des risques

200. Le responsable de la FGR devrait être chargé de fournir à l'organe de direction des informations complètes et compréhensibles sur les risques, ainsi que des conseils, lui permettant 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.
201. 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. S'il n'est pas approprié, 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 combinée 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 combinées. En tout état de cause, cette personne devrait disposer d'une autorité, d'un statut et d'une indépendance suffisants (par exemple le responsable du service juridique).

202. Le responsable de la FGR devrait être en mesure de remettre en cause les décisions prises 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 relative à un crédit ou un investissement ou la fixation d'une limite) prises 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'appel ou de remontée aux échelons supérieurs et les modalités de participation de l'organe de direction.
203. 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 FGM sur des problématiques de risque importantes, y compris les évolutions qui peuvent ne pas être cohérentes avec la stratégie en matière de risque et l'appétit pour le risque de l'établissement.

21 Fonction de vérification de la conformité

204. 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 dans l'ensemble de l'établissement (le responsable de la conformité ou le directeur de la conformité).
205. S'il n'est pas approprié, 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 combinée avec celle du responsable de la FGR ou être exercée par une autre personne titulaire d'un poste supérieur (par exemple le responsable du service juridique), à condition qu'il n'y ait pas de conflits d'intérêts entre les fonctions combinées.
206. La fonction de vérification de la conformité, y compris le responsable de la 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 combinée avec la FGR ou avec d'autres fonctions appropriées, par exemple le service juridique ou les ressources humaines.
207. Le personnel de la fonction de vérification de la conformité devrait disposer de connaissances, de compétences et d'une expérience suffisantes s'agissant de la vérification de la conformité et des procédures pertinentes et devrait avoir accès à une formation régulière.
208. L'organe de direction dans sa fonction de surveillance devrait superviser la mise en œuvre d'une politique bien documentée en matière de vérification de la conformité, qui devrait être

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

209. La fonction de vérification de la conformité devrait fournir à l'organe de direction des conseils sur les mesures à prendre pour garantir la conformité aux lois, règles, règlements et 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.
210. La fonction de vérification de la conformité devrait veiller à ce que la conformité soit surveillée au moyen d'un programme de surveillance clairement défini et structuré 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 en tant que de besoin avec la FGR sur le risque de conformité auquel l'établissement est exposé, ainsi que sur sa gestion. La fonction de vérification de la conformité et la FGR devraient coopérer et échanger des informations en tant que de besoin 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.
211. 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 au cadre juridique actuel et, le cas échéant, aux modifications connues devant bientôt être apportées à la législation, à la réglementation et aux exigences prudentielles.
212. Les établissements devraient prendre des mesures appropriées contre tout comportement interne ou externe susceptible de favoriser ou permettre la fraude, le blanchiment de capitaux, le financement du terrorisme ou d'autres crimes financiers ou manquements à la discipline (par exemple une violation des procédures internes ou un dépassement des limites).
213. Les établissements devraient veiller à ce que leurs filiales et leurs succursales prennent des mesures visant à garantir que leurs opérations respectent les lois et réglementations locales. Si les lois et réglementations locales empêchent l'application de procédures et de systèmes de vérification de la conformité plus stricts mis en œuvre par le groupe, notamment si elles empêchent la divulgation et l'échange des 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

214. 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.
215. La FAI devrait être indépendante des activités contrôlées. La FAI ne devrait donc pas être combinée avec d'autres fonctions.
216. En adoptant une approche fondée sur les risques, la FAI devrait examiner de manière indépendante la conformité de toutes les activités et unités d'un établissement, y compris des activités externalisées, aux politiques et procédures de l'établissement et aux exigences réglementaires, et fournir une assurance objective en la matière. Toute entité au sein du groupe devrait relever de la compétence de la FAI.
217. 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, ou 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 aux règles applicables.
218. La FAI devrait déterminer 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. le fait pour les politiques et procédures existantes de rester ou non adéquates et de respecter ou non les exigences juridiques et réglementaires, ainsi que la stratégie en matière de risque et l'appétit pour le risque de l'établissement ;
 - c. la conformité des procédures aux lois et réglementations applicables et aux décisions de l'organe de direction ;
 - d. la mise en œuvre appropriée et efficace, ou non, des procédures (par exemple la conformité des transactions, le 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.
219. 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 des sources d'information utilisées pour ses modèles internes (par exemple la modélisation des risques et les mesures comptables). Elle devrait également évaluer la qualité et l'utilisation des outils qualitatifs de détection et d'évaluation des risques et les mesures prises pour atténuer les risques.
220. La FAI devrait avoir 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 de l'information et aux procès-verbaux de tous les comités et organes de prise de décisions.
221. La FAI devrait respecter les normes professionnelles nationales et internationales. Les normes professionnelles susmentionnées sont, par exemple, celles établies par l'Institut des auditeurs internes.
222. 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.
223. Un plan d'audit interne devrait être établi au moins une fois par an en fonction des objectifs de contrôle de l'audit interne annuel. Le plan d'audit interne devrait être approuvé par l'organe de direction.
224. Toutes les recommandations relatives à l'audit devraient être soumises à une procédure de suivi formelle aux niveaux hiérarchiques appropriés, afin de garantir leur mise en œuvre effective et en temps utile et afin de rendre des comptes à ce sujet.

Titre VI – Gestion de la continuité des activités⁴⁰

225. Les établissements devraient mettre en place un plan de gestion saine de la continuité de leurs activités et de reprise des activités, afin de garantir leur capacité à fonctionner sans interruption et à limiter les pertes en cas de perturbation grave de leurs activités.
226. Les établissements peuvent instaurer une fonction indépendante spécifique de continuité des activités, par exemple dans le cadre de la FGR⁴¹.

⁴⁰ Les établissements devraient également consulter les orientations de l'ABE sur la gestion des risques liés aux TIC, disponibles à l'adresse <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>

⁴¹ Voir également l'article 312 du règlement (UE) n° 575/2013.

227. L'activité de l'établissement repose sur plusieurs ressources essentielles (par exemple les systèmes informatiques, y compris les services d'informatique en nuage, les systèmes de communication, le personnel stratégique 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 la réputation et d'autres conséquences significatives engendrées par un sinistre ou une indisponibilité prolongée de ces ressources et par la perturbation des procédures opérationnelles ordinaires de l'établissement qui en résulte. D'autres mesures de gestion des risques peuvent consister à réduire la probabilité de ces incidents ou à transférer leur impact financier à des tiers (par exemple en souscrivant une assurance).
228. Afin de mettre en place un plan de gestion saine de la continuité de ses activités, un établissement devrait analyser avec soin les facteurs de risque liés aux perturbations graves de ses activités, ainsi que son exposition à ces perturbations, et évaluer (sur le plan tant quantitatif que qualitatif) leur incidence potentielle au moyen de données internes et/ou externes ou d'une analyse 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.
229. Sur la base de l'analyse susmentionnée, l'établissement devrait mettre en place :
- a. des plans d'urgence 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 conforme à l'appétit pour le risque de l'établissement.
230. Les plans d'urgence, de continuité des activités et de reprise des activités devraient être documentés 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 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

231. 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.

232. En conséquence, l'organe de direction devrait informer les membres du personnel concerné des stratégies et politiques de l'établissement de manière claire et cohérente et tenir 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.
233. 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 inclure toutes les entités au sein de la structure de groupe au sens de la directive 2013/34/UE⁴², par pays.
234. 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 à l'établissement 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.

⁴² 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).

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

Conformément au titre III, les établissements devraient tenir compte des aspects suivants lorsqu’ils documentent les politiques et 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, y compris la façon dont la diversité est prise en compte
 - 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, s’il a été instauré
 - 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
 7. Description de la stratégie en matière de risque et du cadre de gestion des risques
-

8. Structure organisationnelle (avec incidence sur le groupe, le cas échéant)
 - a) structure opérationnelle, lignes d'activité et répartition des compétences et des responsabilités
 - b) externalisation
 - c) gamme de produits et de services
 - d) portée géographique de l'activité
 - e) prestation de services en vertu du principe de la libre prestation de services
 - f) succursales
 - g) filiales, coentreprises, etc.
 - h) utilisation de centres extraterritoriaux
9. 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
10. 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.

