Commission de Surveillance du Secteur Financier

Luxembourg, le 22 décembre 2016

A tous les établissements de crédit, entreprises d'investissement et professionnels effectuant des opérations de prêt

CIRCULAIRE CSSF 16/647

Concerne : Mise à jour de la circulaire CSSF 12/552 relative à l'administration centrale, gouvernance interne et gestion des risques suite à l'adoption des orientations de l'Autorité bancaire européenne (ABE/EBA) en matière de limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013 (EBA/GL/2015/20)

Mesdames, Messieurs,

L'objet de la présente circulaire est de porter à votre attention les orientations de l'Autorité bancaire européenne (ABE/EBA) en matière de limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013[1] (ci-après les « entités shadow banking ») (EBA/GL/2015/20)[2] qui entreront en vigueur le 1er janvier 2017 et que la CSSF s'est engagée à respecter en sa capacité d'autorité compétente.

Les EBA/GL/2015/20 s'appliquent à tous les établissements auxquels s'applique la quatrième partie (« Grands Risques ») du règlement (UE) n° 575/2013 (la « CRR »), conformément au niveau d'application prévu à la première partie, titre II de la CRR.

Lesdites orientations définissent la notion d' « entité shadow banking » et précisent les principes que les établissements doivent observer en matière de gestion et de mesure des risques de crédit, individuels et de concentration, pouvant résulter d'expositions sur des entités shadow banking. Pour ce faire, les orientations précisent les principes de contrôle interne sur lesquels les établissements doivent fonder leur gestion du risque. En complément, les orientations précisent la façon dont les expositions sur des entités shadow banking devraient être traitées dans le contexte de la réglementation relative à la limitation des Grands Risques de la CRR.

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

[2] Les orientations sont disponibles sur le site de l'ABE à l'adresse suivante : https://www.eba.europa.eu/regulation-and-policy/large-exposures/guidelines-on-limits-on-exposures-to-shadow-banking.

Les entités shadow banking sont définies au paragraphe 11 « Définitions » des EBA/GL/2015/20. Il s'agit des entreprises exerçant une ou plusieurs activités d'intermédiation de crédit et qui ne sont pas considérées comme des « entreprises exclues » au sens dudit paragraphe. Par « activités d'intermédiation de crédit », il y a lieu d'entendre les « activités non bancaires comprenant la transformation d'échéances, la transformation de liquidité, le financement d'investissement par effet de levier (leverage) et le transfert de risque de crédit ou des activités similaires ».

Les entités shadow banking visées par les orientations de l'EBA sont notamment :

- toutes les entreprises qui investissent dans des actifs financiers dont l'échéance résiduelle ne dépasse pas deux ans (actifs à court terme) et qui ont pour objectifs distincts ou cumulés d'offrir des rendements comparables à ceux du marché monétaire et/ou de préserver la valeur de l'investissement (les fonds monétaires);
- les fonds d'investissement alternatifs autorisés à consentir des prêts et/ou les entreprises ayant recours à l'effet de levier de manière substantielle;[3]
- les entreprises effectuant au moins les activités énumérées aux points 1 à 3, 6 à 8 et 10 de l'annexe 1 de la Directive 2013/36/UE.

La présente circulaire modifie la circulaire CSSF 12/552 sur les points concernant la gestion des risques. Afin d'en faciliter la lecture et la compréhension, les changements sont présentés en annexe en version « suivi des modifications » (Annexe 1).

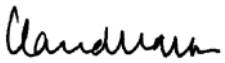
Les EBA/GL/2015/20 entrent en vigueur à dater du 1er janvier 2017. Les établissements sont invités à mettre à jour leurs processus et procédures internes afin de satisfaire à l'ensemble des dispositions des orientations à partir de cette date. Pour le bon ordre, une copie intégrale des orientations est annexée à la présente (Annexe 2).

Veuillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Jean-Pierre FABER	Françoise KAUTHEN	Claude SIMON
Directeur	Directeur	Directeur

[3] Conformément à l'article 111, paragraphe 1, du règlement délégué (UE) n° 231/2013 de la Commission du 19 décembre 2012 complétant la directive 2011/61/UE du Parlement européen et du Conseil en ce qui concerne les dérogations, les conditions générales d'exercice, les dépositaires, l'effet de levier, la transparence et la surveillance.



Simone DELCOURT
Directeur

Claude MARX
Directeur général

Annexe 1
Annexe 2

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Luxembourg, 11 décembre 2012

A tous les établissements de crédit, entreprises d'investissement et professionnels effectuant des opérations de prêt[1]

CIRCULAIRE CSSF 12/552 telle que modifiée par les circulaires CSSF 13/563, CSSF 14/597, ~~et~~ CSSF 16/642 et CSSF 16/647

Concerne: Administration centrale, gouvernance interne et gestion des risques

Mesdames, Messieurs,

Les articles 5 paragraphe 1bis et 17 paragraphe 1bis de la loi du 5 avril 1993 relative au secteur financier exigent des établissements de crédit et des entreprises d'investissement qu'ils disposent d'un solide dispositif de gouvernance interne, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités qui soit bien défini, transparent et cohérent, des processus efficaces de détection, de gestion, de contrôle et de déclaration des risques auxquels ils sont ou pourraient être exposés, des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines et des politiques et pratiques de rémunération permettant et promouvant une gestion saine et efficace des risques, ainsi que des mécanismes de contrôle et de sécurité de leurs systèmes informatiques.

Dans le passé, suivant les développements réglementaires sur le plan international et les nécessités locales, la CSSF avait précisé les modalités d'application de ces articles dans différentes circulaires. L'ajout de nouvelles circulaires transposant les lignes directrices de l'Autorité bancaire européenne (EBA) en matière de gouvernance interne du 27 septembre 2011 (« EBA Guidelines on Internal Governance (GL 44) ») et celles du Comité de Bâle sur le contrôle bancaire (BCBS) en matière d'audit interne du 28 juin 2012 (« The internal audit function in banks ») aurait généré d'importantes redondances et multiplié les terminologies utilisées. Ainsi la CSSF a décidé de concentrer l'ensemble des modalités d'application clé en matière de gouvernance interne dans une circulaire unique. Cette circulaire reprend les lignes directrices de l'EBA et du BCBS mentionnées ci-avant qu'elle complète par les dispositions additionnelles contenues dans les circulaires IML 96/126, IML 98/143, CSSF 04/155, CSSF 05/178 et CSSF 10/466[2].

---

[1] Pour les professionnels effectuant des opérations de prêt, tels que définis à l'article 28-4 de la loi du 5 avril 1993 relative au secteur financier, seul le chapitre 3 de la partie III est applicable.

[2] Circulaires IML 96/126 concernant l'organisation administrative et comptable, IML 98/143 concernant le contrôle interne, CSSF 04/155 concernant la fonction compliance, CSSF 05/178 concernant l'organisation administrative et

Par ailleurs, afin de présenter une vue d'ensemble, la circulaire reprend, par référence aux articles 5 paragraphe 1 et 17 paragraphe 1 de la loi du 5 avril 1993 relative au secteur financier, les modalités d'application en matière d'administration centrale telles que précisées dans la circulaire IML 95/120.

En conséquence, les circulaires IML 95/120, IML 96/126, IML 98/143, CSSF 04/155, CSSF 05/178 et CSSF 10/466 sont abrogées dans le chef des établissements de crédit et entreprises d'investissement.[3]

Finalement, la circulaire entend recueillir également l'ensemble des dispositions en matière de gestion des risques.

La présente circulaire constitue un premier pas vers un recueil réglementaire consolidé en matière de gouvernance interne au sens large. Elle ne comprend pas l'ensemble des domaines visés, comme par exemple celui de la rémunération qui est couvert par le référentiel CRD (« Capital Requirements Directive » - circulaires CSSF 06/273 et CSSF 07/290) et par la circulaire CSSF 11/505 donnant des précisions relatives au principe de proportionnalité en matière de rémunération.

Le même constat s'applique aux risques. La présente circulaire se limite pour l'essentiel à transposer des lignes directrices du CEBS ainsi que des orientations de l'EBA. Il s'agit des lignes directrices du 2 septembre 2010 en matière de risques de concentration (« CEBS Guidelines on the management of concentration risk under the supervisory review process (GL31) »), ~~et~~ des lignes directrices du 27 octobre 2010 en matière de tarification de la liquidité (« Guidelines on Liquidity Cost Benefit Allocation »), des orientations de l'EBA du 22 mai 2015 sur la gestion du risque de taux d'intérêt inhérent aux activités autres que de négociation (« Guidelines on the management of interest rate risk arising from non-trading activities » - EBA/GL/2015/08) et des ~~–~~orientations de l'EBA du 14 décembre 2015 sur les limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013 (« Guidelines on the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) n° 575/2013 » - EBA/GL/2015/20). En outre, la circulaire reprend les principes de prudence de base dans le domaine de l'octroi des crédits et de la gestion patrimoniale privée.

Pour ce qui concerne les établissements CRR,[4] la présente circulaire doit se lire en parallèle avec le Règlement CSSF n° 15-02 relatif au processus de contrôle et d'évaluation prudentiels s'appliquant aux établissements CRR.

Les multiples circulaires existantes relatives aux risques et à leur gestion seront rassemblées au sein d'une version ultérieure de la présente circulaire.

---

comptable et la sous-traitance en matière informatique et CSSF 10/466 concernant les informations à publier en situations de crise.

[3] Les circulaires IML 95/120, IML 96/126, IML 98/143 et CSSF 05/178 restent en vigueur pour les PSF qui ne sont pas des entreprises d'investissement. Ces circulaires, ensemble avec la circulaire CSSF 04/155, restent d'application pour les établissements de paiement et les établissements de monnaie électronique.

[4] Le terme « établissement CRR » est défini à l'article 1er, paragraphe 1 du Règlement CSSF n° 15-02.

Lorsqu'en réponse à des développements réglementaires sur le plan international ou des nécessités locales, la CSSF est amenée à préciser les exigences reprises dans la présente circulaire, elle procédera à la mise à jour de cette circulaire. La partie IV de la circulaire contient une chronologie des mises à jour qui permet au lecteur de retracer les modifications opérées par les mises à jour successives.

La circulaire est divisée en quatre parties : la première contient le champ d'application, la deuxième les exigences de structure en matière d'administration centrale et de gouvernance interne, la troisième les exigences spécifiques en matière de gestion des risques et la quatrième l'entrée en vigueur et les mesures transitoires et dispositions abrogatoires. La table des matières se présente comme suit.

Les encadrés qui apparaissent dans la circulaire contiennent des remarques et précisions qui servent d'orientation pour la mise en œuvre des exigences contenues dans la présente circulaire.

Table des matières

Partie I. Définitions et champ d'application

Chapitre 1. Définitions

1. On entend aux fins de la présente circulaire par :

   1) « conseil d'administration » : l'organe ou à défaut les personnes qui du point de vue du droit des sociétés contrôlent la gestion exercée par la direction autorisée. Le terme n'est pas à prendre dans son acceptation juridique, puisque les banques et entreprises d'investissement peuvent revêtir une forme juridique qui ne prévoit pas de « conseil d'administration » au sens du droit des sociétés. Par exemple, en présence d'un conseil de surveillance, ce dernier assumera les responsabilités que la présente circulaire attribue au « conseil d'administration » ;

   2) « direction autorisée » : les personnes visées aux articles 7 paragraphe 2 et 19 paragraphe 2 de la loi du 5 avril 1993 relative au secteur financier. Ces personnes sont désignées par « directeurs autorisés » ;

   3) « établissement » : une entité telle que définie au chapitre 2 de la partie I ;

   4) « fonction clé » : toute fonction dont l'exercice permet d'avoir une influence notable sur la conduite ou le contrôle des activités. Ces fonctions clé comprennent au minimum les administrateurs, directeurs autorisés et les responsables des trois fonctions de contrôle interne suivant le point 105 (c'est-à-dire la fonction de contrôle des risques, la fonction compliance et la fonction d'audit interne);

   5) « LSF » : la loi du 5 avril 1993 relative au secteur financier ;

   6) « parties liées » : les entités juridiques appartenant au groupe auquel l'établissement appartient ainsi que les employés, actionnaires, directeurs et membres du conseil d'administration de ces entités.

Chapitre 2. Champ d'application

2. La présente circulaire s'applique aux établissements de crédit et aux entreprises d'investissement de droit luxembourgeois, y compris à leurs succursales, ainsi qu'aux succursales luxembourgeoises d'établissements de crédit et d'entreprises d'investissement dont l'origine se situe en dehors de l'Espace économique européen. Pour les domaines où la CSSF conserve une responsabilité de contrôle en tant qu'autorité d'accueil – il s'agit des mesures en matière de lutte contre le blanchiment et le financement du terrorisme, de marchés d'instruments financiers et de la liquidité - les succursales luxembourgeoises d'établissements de crédit et d'entreprises d'investissement originaires d'un Etat membre de l'Espace économique européen mettent en place un dispositif en matière d'administration centrale et de gouvernance interne ainsi qu'une gestion des risques qui sont comparables à ceux prescrits par la présente circulaire.

   Toutes les entités visées aux paragraphes précédents sont désignées ci-après par le terme « établissements ».

   En ce qui concerne les professionnels effectuant des opérations de prêt, tels que définis à l'article 28-4 de la LSF, seul le chapitre 3 de la partie III de la présente circulaire est applicable.

Le chapitre 6 de la partie III de la présente circulaire s'applique uniquement aux établissements de crédit.

3. La circulaire s'applique aux établissements sur base individuelle et consolidée.

   Lorsqu'il existe des entités juridiques, consolidées ou non, pour lesquelles l'établissement est entreprise mère au sens de la LSF, le terme « établissement » sert à désigner le « groupe », c'est-à-dire l'ensemble formé par l'entreprise mère (la « tête de groupe ») et les entités juridiques pour lesquelles l'établissement est entreprise mère au sens de la LSF. La circulaire s'applique alors au « groupe » dans son ensemble, aux différentes entités juridiques qui le composent, y compris leurs succursales éventuelles, ainsi qu'aux relations entre ces entités juridiques, dans le respect des lois et des dispositions réglementaires nationales qui s'appliquent aux entités juridiques en question.

   Dans le cas d'entités juridiques dans lesquelles l'établissement détient une participation entre 20% et 50% mais pour lesquelles l'établissement n'est pas entreprise mère au sens de la LSF, l'établissement tête de groupe fait tout son possible, de concert avec les autres actionnaires ou associés concernés, pour que soit mis en place dans ces entités juridiques un dispositif en matière d'administration centrale et de gouvernance interne ainsi qu'une gestion des risques qui répondent à des standards comparables à ceux prescrits par la présente circulaire et dans le respect des lois et des dispositions réglementaires applicables aux niveaux nationaux.

   Quelle que soit la structure organisationnelle et opérationnelle de l'établissement, la mise en œuvre de la présente circulaire permet à l'établissement d'avoir une maîtrise complète de ses activités et des risques auxquels il est exposé ou pourrait être exposé, peu importe la localisation de ces activités et risques.

4. Les mesures d'exécution que les établissements prennent en vertu de la présente circulaire sont proportionnelles à la nature, à l'échelle et à la complexité des activités, y compris les risques, et de l'organisation de l'établissement.

   En pratique, l'application du principe de proportionnalité conduit les établissements qui sont plus importants, complexes ou risqués à se doter d'un dispositif renforcé en matière d'administration centrale et de gouvernance interne. Ce dispositif comprend par exemple l'instauration de comités spécialisés suivant la section 4.1.4. A l'opposé, pour des établissements dont la diversité, la taille ou la complexité de l'activité sont moindres, le principe de proportionnalité peut jouer à la baisse. Ainsi ces établissements peuvent fonctionner adéquatement au sens de la présente circulaire avec des fonctions compliance et de contrôle des risques assumées à temps partiel (voir les points 129 et 141), avec un audit interne sous-traité (point 117) ou encore moyennant le recours à des experts externes en vue de réaliser certaines tâches de contrôle interne (point 118). L'application à la baisse du principe de proportionnalité est limitée en particulier par le principe de la ségrégation des tâches qui exige que les tâches et responsabilités doivent être attribuées de façon à éviter les conflits d'intérêts dans le chef d'une même personne (voir le point 71). Au niveau de la direction autorisée, ce principe est atténué par le principe de la responsabilité collective de la direction autorisée (voir le point 72). Alors que la répartition des tâches au niveau de la direction autorisée s'effectue dans le respect du principe de la ségrégation des tâches, la responsabilité reste collective. Par application du principe de proportionnalité, lorsqu'un établissement ne nécessite pas

plus que deux directeurs autorisés, la répartition efficace des tâches n'est pas toujours compatible avec une ségrégation stricte des tâches au niveau de cette direction. Par exemple, il est admissible dans ce cas de figure que le même membre de la direction autorisée soit en charge à la fois de l'organisation administrative, comptable et informatique et des fonctions de contrôle interne (voir le point 63). Quelle que soit l'organisation retenue, les arrangements en la matière permettent à l'établissement d'opérer dans le plein respect des dispositions prévues au chapitre 3 de la partie II.

Partie II. Dispositif en matière d'administration centrale et de gouvernance interne

Chapitre 1. L'administration centrale

5. Les établissements disposent au Luxembourg d'une solide administration centrale, comportant leur « centre de prise de décision » et leur « centre administratif ». L'administration centrale, qui englobe au sens large les fonctions de direction et de gestion, d'exécution et de contrôle, permet à l'établissement d'avoir la maîtrise de l'ensemble de ses activités.

6. La notion de centre de prise de décision ne comprend pas seulement l'activité de la direction autorisée suivant les articles 7 paragraphe 2 et 19 paragraphe 2 de la LSF, mais également celle des responsables des différentes fonctions commerciales, de support et de contrôle ou des différentes unités opérationnelles (services, départements ou métiers) existant à l'intérieur de l'établissement.

7. Le centre administratif comprend en particulier une bonne organisation administrative, comptable et informatique qui assure en permanence la bonne administration des valeurs et des biens, l'exécution adéquate des opérations, l'enregistrement correct et exhaustif des opérations et la production d'une information de gestion correcte, complète, pertinente, compréhensible et disponible sans délais. Il inclut à ce titre l'infrastructure administrative des fonctions commerciales (section 5.2.1), les fonctions de support, en particulier dans le domaine financier et comptable (section 5.2.2) et informatique (section 5.2.3), ainsi que le contrôle interne (chapitre 6).

8. Lorsque l'établissement est tête de groupe suivant le point 3, l'administration centrale permet à l'établissement de concentrer en son siège à Luxembourg toute l'information de gestion nécessaire pour gérer, suivre et contrôler de façon continue les activités du groupe. De même, l'administration centrale permet à l'établissement d'atteindre toutes les entités juridiques et succursales qui composent le groupe afin de leur fournir toute l'information de gestion nécessaire. La notion d'information de gestion s'entend au sens le plus large, incluant l'information financière et le reporting prudentiel.

Chapitre 2. Le dispositif de gouvernance interne

9. La gouvernance interne est une composante limitée mais cruciale de la gouvernance d'entreprise, se concentrant sur la structure interne et l'organisation d'un établissement. La gouvernance d'entreprise est un concept plus vaste qui peut être décrit comme étant l'ensemble des relations entre un établissement, son conseil

d'administration, sa direction autorisée, ses actionnaires et les autres parties prenantes.

La gouvernance interne doit assurer en particulier la gestion saine et prudente des activités, y compris des risques qui leur sont inhérents. Afin d'atteindre cet objectif, les établissements mettent en place un dispositif de gouvernance interne qui répond au concept des « trois lignes de défense » (« three-lines-of-defence model »).

La première ligne de défense est constituée par les unités opérationnelles qui prennent ou acquièrent des risques dans le cadre d'une politique et de limites prédéfinies et qui effectuent des contrôles tels que décrits en particulier à la section 6.1.1.

La seconde ligne est formée par les fonctions de support, y compris la fonction financière et comptable (section 5.2.2) ainsi que la fonction informatique (section 5.2.3), et les fonctions compliance et de contrôle des risques (sous-chapitre 6.2 et sections 6.2.5 et 6.2.6) qui contribuent au contrôle indépendant des risques.

La troisième ligne est constituée par la fonction d'audit interne qui, conformément au sous-chapitre 6.2 et à la section 6.2.7, effectue une évaluation indépendante, objective et critique des deux premières lignes de défense.

Les trois lignes de défense sont complémentaires, chaque ligne de défense assumant ses responsabilités de contrôle indépendamment des autres lignes. Les contrôles réalisés par les trois lignes de défense comprennent les quatre niveaux de contrôles prévus au point 100.

10. Concrètement, et dans le but de respecter les objectifs définis au point précédent, le dispositif de gouvernance interne comprend notamment :

- une structure organisationnelle et opérationnelle claire et cohérente comportant des pouvoirs de décision, des liens hiérarchiques et fonctionnels et un partage des responsabilités clairement définis, transparents, cohérents, complets et exempts de conflits d'intérêts (sous-chapitres 5.1, 7.1 et 7.2);
- des mécanismes adéquats de contrôle interne qui répondent aux dispositions du chapitre 6. Ces mécanismes comprennent des procédures administratives, comptables et informatiques saines et des politiques et pratiques de rémunération permettant et promouvant une gestion saine et efficace des risques par application des règles contenues dans les circulaires CSSF 06/273, CSSF 07/290 et CSSF 11/505, en ligne avec la stratégie de l'établissement en matière de risques, ainsi que des mécanismes de contrôle et de sécurité des systèmes d'information de gestion. La notion de système d'information de gestion comprend les systèmes informatiques (sections 5.2.1 à 5.2.3, sous-chapitres 5.3 et 7.4);
- une procédure formelle d'escalade, de règlement et, le cas échéant, de sanctions pour les problèmes, déficiences et irrégularités relevés par le biais des mécanismes de contrôle interne, y compris les fonctions de contrôle interne suivant le sous-chapitre 6.2 ;
- des processus de détection, de mesure, de déclaration, de gestion et d'atténuation ainsi que de contrôle des risques auxquels les établissements sont ou pourraient être exposés conformément au chapitre 1 de la partie III ;

- un système d'information de gestion, y compris en matière de risques, ainsi qu'un dispositif de communication interne comprenant un dispositif interne d'alerte (« whistleblowing ») qui permet au personnel de l'établissement d'attirer l'attention des responsables sur toutes leurs préoccupations importantes et légitimes liées à la gouvernance interne de l'établissement (section 5.2.4);
- un dispositif de gestion de continuité des activités visant à limiter les risques de perturbation grave des activités et à assurer le maintien des opérations clé telles que définies par le conseil d'administration sur proposition de la direction autorisée. Ce dispositif comprend un plan de continuité qui décrit les actions à mettre en œuvre afin de poursuivre les activités en cas d'incident ou sinistre (sections 5.2.3 et 7.4);
- un dispositif de gestion de crises qui assure une capacité de réaction appropriée en cas de crise, y compris un plan de rétablissement des activités. Ce dispositif satisfait aux exigences énoncées à la section 5.2.5.

11. Les établissements promeuvent une culture interne du contrôle et du risque qui vise à assurer que tout le personnel de l'établissement participe activement au contrôle interne ainsi qu'à la détection, à la déclaration et au contrôle des risques encourus par l'établissement et adopte une attitude positive à l'égard du contrôle interne tel que défini au chapitre 6.

Chapitre 3. Propriétés génériques d'un dispositif « solide » en matière d'administration centrale et de gouvernance interne

12. Le dispositif en matière d'administration centrale et de gouvernance interne est élaboré et mis en œuvre de sorte à ce qu'il

- fonctionne de manière intègre (« intégrité »). Ce volet inclut aussi bien la gestion des conflits d'intérêts que la sécurité, en particulier en matière de systèmes d'information;
- soit fiable et fonctionne de manière continue (« robustesse »). En vertu du principe de continuité, les établissements se dotent également d'arrangements visant à rétablir le fonctionnement du dispositif de gouvernance interne en cas de discontinuité;
- soit efficace (« efficacité »). L'efficacité s'apprécie en particulier au fait que les risques sont effectivement gérés et contrôlés;
- réponde aux besoins de l'établissement dans son ensemble et de toutes ses unités organisationnelles et opérationnelles (« adéquation »);
- soit cohérent dans son ensemble et dans ses parties (« cohérence »);
- soit complet (« exhaustivité »). En ce qui concerne les risques, l'exhaustivité signifie que l'ensemble des risques doit être inclus dans le périmètre du dispositif de gouvernance interne. Ce périmètre ne s'arrête pas (nécessairement) au seul périmètre (consolidé) prudentiel ou comptable ; il doit permettre à l'établissement de disposer d'une vue exhaustive sur tous ses risques, en termes de leur substance économique, en tenant compte de toutes les interactions existant à travers l'établissement. S'agissant du contrôle

interne, le principe d'exhaustivité implique que le contrôle interne porte sur tous les domaines du fonctionnement de l'établissement;

- soit transparent (« transparence »). La transparence comprend une attribution et une communication claires et visibles des rôles et des responsabilités aux différents membres du personnel, à la direction autorisée et aux unités opérationnelles et organisationnelles de l'établissement.

13. En exécution d'un organigramme (sous-chapitre 5.1), l'établissement dispose au siège luxembourgeois, dans ses succursales ainsi que dans l'ensemble des différentes entités juridiques qui composent le groupe, de ressources humaines suffisantes en nombre et disposant d'une compétence professionnelle individuelle et collective appropriée, ainsi que de l'infrastructure administrative et technique nécessaire et suffisante pour pouvoir exercer les activités qu'il veut réaliser. Ces ressources humaines et cette infrastructure respectent les dispositions des sous-chapitres 5.1 et 5.2.

    La sous-traitance est possible dans les conditions énoncées au sous-chapitre 7.4.

14. Les établissements documentent par écrit l'ensemble du dispositif en matière d'administration centrale et de gouvernance interne ainsi que l'ensemble de leurs activités (opérations et risques) conformément au sous-chapitre 5.3.

15. En vue d'assurer et de maintenir la solidité du dispositif en matière d'administration centrale et de gouvernance interne, ce dernier fait l'objet d'une révision objective, critique et régulière, au moins une fois par an. Cette révision tient compte de tous les changements internes et externes qui peuvent avoir une influence significative défavorable sur la solidité de ce dispositif dans son ensemble et sur le profil de risque et la capacité de l'établissement à gérer et à supporter ses risques en particulier.

16. Les établissements publient les éléments clé de leur dispositif de gouvernance interne dans le respect des règles régissant la partie XIX de la circulaire CSSF 06/273 (« pilier 3 »). Cette publication inclut la structure organisationnelle et opérationnelle, y compris en matière de contrôle interne, la stratégie en matière de risques ainsi que le profil de risque. Ces informations décrivent la situation actuelle et son évolution attendue d'une manière claire, objective et pertinente.

Chapitre 4. Conseil d'administration et direction autorisée

Sous-chapitre 4.1. Le conseil d'administration

Section 4.1.1. Responsabilités du conseil d'administration

17. Le conseil d'administration a la responsabilité globale de l'établissement. Il veille à faire assurer l'activité et à préserver la continuité de l'activité au moyen d'un solide dispositif en matière d'administration centrale et de gouvernance interne conformément aux dispositions de la présente circulaire. A cette fin, le conseil d'administration approuve et arrête par écrit, dans le respect des dispositions légales et réglementaires et après avoir entendu la direction autorisée et les responsables des fonctions de contrôle interne, et dans le but de protéger l'établissement et sa réputation, notamment

- la stratégie commerciale (modèle d'activités) de l'établissement dans le respect des intérêts financiers de l'établissement à long terme, de sa solvabilité et de sa situation des liquidités;
- la stratégie de l'établissement en matière de risques, y compris la tolérance au risque et les principes directeurs régissant la détection, la mesure, la déclaration, la gestion et le contrôle des risques;
- la stratégie de l'établissement en matière de fonds propres et de liquidités réglementaires et internes;
- les principes directeurs d'une structure organisationnelle et opérationnelle claire et cohérente qui règle en particulier la création et le maintien par l'établissement d'entités (structures) juridiques, ainsi que les principes directeurs en matière de systèmes d'informations, y compris l'aspect sécurité, et de dispositif de communication interne, y compris le dispositif interne d'alerte;
- les principes directeurs relatifs aux mécanismes de contrôle interne qui incluent les fonctions de contrôle interne et la politique de rémunération, les principes directeurs en matière d'escalade, de règlement et de sanctions visant à assurer que tout comportement non respectueux de règles applicables soit adéquatement poursuivi et sanctionné, ainsi que les principes directeurs en matière de déontologie (« code de conduite interne») et de valeurs d'entreprise, y compris dans le domaine de la gestion des conflits d'intérêts;
- les principes directeurs en matière d'administration centrale au Luxembourg, comprenant les moyens humains et matériels que nécessite la mise en œuvre de la structure organisationnelle et opérationnelle ainsi que des stratégies de l'établissement, les principes directeurs en matière d'organisation administrative, comptable et informatique, les principes directeurs en matière de sous-traitance (« outsourcing ») ainsi que les principes directeurs régissant la modification de l'activité (en termes de couverture de marchés et de clientèle, de nouveaux produits et de services) et l'approbation et le maintien d'activités « inhabituelles » ou « non transparentes »;
- les principes directeurs applicables en matière de dispositif de gestion de continuité des activités et de gestion de crises et
- les principes directeurs régissant la nomination et la succession aux fonctions clé de l'établissement, ainsi que les procédures régissant le conseil d'administration en termes de sa composition, de ses responsabilités, de son organisation et de son fonctionnement.[5] Les principes directeurs régissant la nomination et la succession aux fonctions clé de l'établissement stipulent qu'en la matière, l'établissement doit se conformer aux exigences de la présente circulaire, à la procédure prudentielle d'approbation des titulaires de fonctions clé telle que publiée sur le site internet de la CSSF ainsi qu'aux orientations publiées par l'EBA le 22 novembre 2012 (*Guidelines on the*

[5] Dans le respect de la gouvernance d'entreprise, les principes directeurs et procédures applicables aux membres du conseil d'administration sont à soumettre le cas échéant aux actionnaires pour accord.

assessment of the suitability of members of the management body and key function holders - EBA/GL/2012/06).

Remarque :

Les orientations de l'EBA en matière d'évaluation de l'aptitude des titulaires de fonctions clé prévoient en particulier que les établissements :

- identifient l'ensemble des fonctions clé (voir aussi le point 1 à ce sujet);
- définissent les critères (en termes d'honorabilité, de compétences professionnelles et de qualités personnelles) qu'ils mettent en œuvre afin d'apprécier l'aptitude des titulaires des fonctions clé. Ces critères sont conformes aux critères prévus aux points 13 à 15 de l'orientation précitée de l'EBA ;
- exigent que les titulaires des fonctions clé soient honorables et présentent les compétences professionnelles et qualités personnelles nécessaires à l'exécution de leur mandat ;
- évaluent par écrit l'aptitude des titulaires de fonctions clé, préalablement à leur nomination, régulièrement au cours de leur mandat et sur base ad hoc lorsqu'une telle réévaluation s'impose ;
- définissent des politiques et procédures relatives à la sélection des titulaires de fonctions clé qui respectent les principes d'une solide gouvernance interne (conformément aux points 7 et 8 de l'orientation précitée de l'EBA).

18. Le conseil d'administration charge la direction autorisée de mettre en œuvre les stratégies et principes directeurs en matière de gouvernance interne visés au point 17 par le biais de politiques et de procédures internes écrites, à l'exception des principes directeurs qui régissent la nomination et la succession au conseil d'administration.

19. Le conseil d'administration surveille la mise en œuvre par la direction autorisée de ses stratégies et principes directeurs en matière de gouvernance interne. A cette fin, il doit notamment approuver les politiques que la direction autorisée arrête en vertu du point 18.

20. Le conseil d'administration évalue d'une manière critique et approuve à des intervalles réguliers, et au moins une fois par an, le dispositif de gouvernance interne de l'établissement. Ces évaluations et approbations visent à assurer que le dispositif de gouvernance interne continue à répondre aux exigences de la présente circulaire et aux objectifs d'une gestion efficace, saine et prudente des activités.

    L'évaluation et l'approbation par le conseil d'administration portent en particulier sur :

    - l'adéquation entre les risques encourus, la capacité de l'établissement à gérer ces risques et les fonds propres et réserves de liquidités internes et réglementaires, compte tenu des stratégies et principes directeurs fixés par le

conseil d'administration et la réglementation existante et notamment la circulaire CSSF 11/506;

- les stratégies et principes directeurs en vue de les améliorer et de les adapter aux changements internes et externes, actuels et anticipés, ainsi qu'aux enseignements tirés du passé;
- la manière dont la direction autorisée s'acquitte des responsabilités énoncées au sous-chapitre 4.2. Dans ce contexte, le conseil d'administration veille en particulier à ce que la direction autorisée mette en œuvre de manière prompte et efficace les mesures correctrices requises pour remédier aux problèmes, déficiences et irrégularités relevés par les fonctions de contrôle interne, le réviseur d'entreprises agréé et la CSSF, conformément aux deux derniers paragraphes du point 57;
- l'adéquation de la structure organisationnelle et opérationnelle. Le conseil d'administration doit avoir une compréhension parfaite de la structure organisationnelle de l'établissement, en particulier en termes des entités (structures) juridiques sous-jacentes, de leur raison d'être, des liens et interactions intra-groupe qui les relient ainsi que des risques y liés. Il vérifie que la structure organisationnelle et opérationnelle correspond aux stratégies et principes directeurs visés au point 17, qu'elle permet une gestion saine et prudente des activités qui est exempte d'opacité et de complexité indue, et qu'elle reste justifiée par rapport aux objectifs assignés. Cette exigence s'applique tout particulièrement aux activités « inhabituelles » ou « non transparentes »;
- l'efficacité et l'efficience des mécanismes de contrôle interne mis en place par la direction autorisée.

Les évaluations en question peuvent être préparées par les comités mis en place par application du point 33. Elles se font en particulier sur base des informations reçues de la part de la direction autorisée (point 61), des rapports de révision émis par le réviseur d'entreprises agréé (rapports sur les comptes annuels, comptes rendus analytiques et, le cas échéant, « management letters »), du rapport ICAAP (point 61) et des rapports de synthèse des fonctions de contrôle interne (point 116) que le conseil d'administration est appelé à approuver à cette occasion.

21. Il appartient au conseil d'administration de promouvoir une culture interne en matière de risque qui sensibilise le personnel de l'établissement aux impératifs d'une gestion saine et prudente des risques et qui favorise une attitude positive à l'égard du contrôle interne et de la compliance et de stimuler le développement d'un dispositif de gouvernance interne qui permet d'atteindre ces objectifs.

    S'agissant des fonctions de contrôle interne, le conseil d'administration veille à ce que les travaux de ces fonctions soient exécutés suivant des normes reconnues. Par ailleurs, le conseil d'administration approuve le plan d'audit interne conformément au point 151.

22. Lorsque le conseil d'administration prend connaissance que le dispositif en matière d'administration centrale ou de gouvernance interne ne permet plus une gestion saine et prudente des activités ou que les risques encourus ne sont ou ne seront plus adéquatement supportés par la capacité de l'établissement à gérer ces risques, par des fonds propres ou des réserves de liquidités réglementaires ou internes, il exige

de la direction autorisée de lui présenter sans délais des mesures correctrices et en informe immédiatement la CSSF. L'obligation de notification à la CSSF porte aussi sur toutes les informations qui remettent en cause la qualification ou l'honorabilité d'un membre du conseil d'administration ou de la direction autorisée ou d'un responsable d'une fonction de contrôle interne.

Section 4.1.2. Composition et qualification du conseil d'administration

23. Les membres du conseil d'administration doivent être suffisants en nombre et présenter dans leur ensemble une composition adéquate qui permet au conseil d'administration de s'acquitter pleinement de toutes ses responsabilités. Le caractère adéquat se réfère en particulier aux compétences professionnelles (connaissances, compréhension et expérience), ainsi qu'aux qualités personnelles des membres du conseil d'administration. Par ailleurs chaque membre doit justifier son honorabilité professionnelle. Les principes directeurs régissant l'élection et la succession des administrateurs expliquent et arrêtent les facultés jugées nécessaires en vue d'assurer une composition et une qualification appropriée du conseil d'administration.

24. Le conseil d'administration doit disposer dans son ensemble d'une compétence appropriée à la nature, à l'échelle et à la complexité des activités et de l'organisation de l'établissement.

    Le conseil d'administration, en tant que collectif, doit avoir une compréhension parfaite de l'ensemble des activités (et des risques qui leur sont inhérents) ainsi que de l'environnement économique et réglementaire dans lequel évolue l'établissement.

    Les membres du conseil d'administration disposent individuellement d'une parfaite compréhension du dispositif de gouvernance interne et de leurs responsabilités au sein de l'établissement. Ils maîtrisent les activités qui sont du ressort de leur domaine d'expertise et disposent d'une bonne compréhension des autres activités significatives de l'établissement.

25. Les membres du conseil d'administration veillent à ce que leurs qualités personnelles leur permettent d'exécuter leur mandat d'administrateur de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance requis. A ce titre, le conseil d'administration ne peut pas compter parmi ses membres une majorité de personnes qui assument un rôle exécutif au sein de l'établissement (directeurs autorisés ou autres employés de l'établissement, à l'exception des représentants du personnel).

    Les membres du conseil d'administration veillent à ce que leur mandat d'administrateur soit et reste compatible avec leurs autres emplois et intérêts éventuels, en particulier en termes de conflits d'intérêts et de disponibilité. Ils informent le conseil d'administration des mandats qu'ils ont en dehors de l'établissement.

26. Les termes des mandats d'administrateur doivent être fixés de manière à permettre au conseil d'administration d'exercer ses responsabilités de manière continue et efficace. La reconduction d'administrateurs existants doit s'orienter en particulier à leurs performances passées. La continuité du fonctionnement du conseil d'administration doit être assurée.

27. Les principes directeurs régissant la nomination et la succession des membres du conseil d'administration prévoient les mesures nécessaires pour que ces membres soient et restent qualifiés tout au long de leur mandat. Ces mesures comprennent des formations professionnelles qui permettent aux membres du conseil d'administration de mettre à jour et d'approfondir leurs compétences requises.

Section 4.1.3. Organisation et fonctionnement du conseil d'administration

28. Le conseil d'administration se réunit régulièrement en vue de s'acquitter de manière efficace de ses responsabilités.

29. Les travaux du conseil d'administration doivent être documentés par écrit. Cette documentation inclut l'agenda des réunions, les procès-verbaux des réunions ainsi que les décisions et mesures prises par le conseil d'administration.

30. Le conseil d'administration évalue régulièrement les procédures régissant le conseil d'administration, son mode de fonctionnement et ses travaux en vue de les améliorer, d'en assurer l'efficacité et de vérifier si les procédures qui lui sont applicables sont respectées dans la pratique.

31. Il appartient au président du conseil d'administration de promouvoir au sein du conseil d'administration une culture de discussion informée et contradictoire et de proposer l'élection d'administrateurs indépendants. Un administrateur indépendant est un administrateur qui ne connaît pas de conflit d'intérêts, de nature à altérer sa capacité de jugement du fait qu'il est lié par une relation d'affaires - familiale ou autre[6] - avec l'établissement, l'actionnaire qui le contrôle ou la direction de l'un ou de l'autre.

    La CSSF recommande aux grands établissements d'avoir un ou plusieurs administrateurs indépendants.

32. Les mandats de directeur autorisé et de président du conseil d'administration ne sont pas cumulables.

Section 4.1.4. Comités spécialisés

33. En vue d'accroître son efficacité, le conseil d'administration peut se faire assister par des comités spécialisés dans le domaine notamment de l'audit, des risques, de la rémunération, des ressources humaines (notamment à travers l'intervention d'un comité de nomination des personnes occupant une fonction clé) ainsi que de la gouvernance interne, de la déontologie et de la compliance lorsque la nature, l'échelle et la complexité de l'établissement et de ses activités l'exigent. Ces comités comprennent des administrateurs qui ne font pas partie de la direction autorisée ni du personnel de l'établissement. Ils peuvent également comprendre, au besoin, des experts externes, indépendants de l'établissement. Leur mission consiste à fournir au conseil d'administration des appréciations critiques concernant l'organisation et le fonctionnement de l'établissement dans les domaines précités en vue de permettre aux membres du conseil d'administration d'exercer de manière efficace leur mission de surveillance et d'assumer leurs responsabilités en vertu de la présente circulaire.

[6] Y inclus une relation salariale

34. Le conseil d'administration fixe par écrit le mandat, la composition et les procédures de travail des comités spécialisés. En vertu de ces procédures, les comités spécialisés doivent pouvoir demander tout document et toute information qu'ils jugent utiles pour l'exercice de leur mission. Par ailleurs, les procédures prévoient les conditions dans lesquelles le réviseur d'entreprises agréé ainsi que toute personne appartenant à l'établissement, y compris la direction autorisée, sont associés aux travaux des comités spécialisés.

35. Le conseil d'administration veille à ce que les différents comités interagissent efficacement et rapportent régulièrement au conseil d'administration. Le conseil d'administration ne peut pas déléguer aux comités spécialisés ses pouvoirs de décision et responsabilités en vertu de la présente circulaire.

36. Les comités spécialisés sont présidés par un de leurs membres. Ces présidents de comité disposent de connaissances approfondies dans le domaine d'activité du comité qu'ils président.

37. Lorsque le conseil d'administration ne se fait pas assister par des comités spécialisés, les tâches énoncées aux sous-sections 4.1.4.1 et 4.1.4.2 incombent directement au conseil d'administration.

Sous-section 4.1.4.1. Le comité d'audit[7]

38. Le comité d'audit a pour objet d'assister le conseil d'administration dans les domaines de l'information financière, du contrôle interne, y compris l'audit interne, ainsi que du contrôle par le réviseur d'entreprises agréé.

39. La CSSF recommande aux grands établissements de créer un comité d'audit afin de faciliter le contrôle effectif des activités par le conseil d'administration.

    Le comité d'audit comprend au moins trois membres et sa composition est déterminée en accord avec ses missions et son mandat conformément aux points 33 et 34. Les compétences collectives des membres du comité d'audit doivent être représentatives des activités et des risques de l'établissement et comprendre des compétences spécifiques en matière d'audit et de comptabilité. Le comité d'audit peut associer à ses travaux la direction autorisée, le responsable de la fonction d'audit interne ainsi que le réviseur d'entreprises agréé de l'établissement. Ces personnes peuvent assister aux réunions du comité ; elles n'en sont pas membres.

40. Le fonctionnement du comité d'audit, en particulier en termes de fréquence et de durée des réunions, est déterminé en fonction de son mandat et de sa mission d'assister le conseil d'administration.

41. Le comité d'audit confirme la charte d'audit interne (point 144). Il apprécie si les moyens humains et matériels engagés au niveau de l'audit interne sont suffisants et s'assure que les auditeurs internes possèdent les compétences nécessaires (point 111) et que l'indépendance de la fonction d'audit interne est sauvegardée.

42. Le comité d'audit confirme le plan d'audit interne (point 151) approuvé par la direction autorisée. Il prend connaissance des informations sur l'état du contrôle

[7] Pour les établissements qui doivent se doter d'un comité d'audit conformément à la loi du 18 décembre 2009 relative à la profession de l'audit, la présente circulaire s'applique sans préjudice des dispositions codifiées à l'article 74 (« Comité d'audit ») de cette loi.

interne que lui fournit la direction autorisée selon une fréquence au moins annuelle en vertu du point 61 de la présente circulaire.

43. Le comité d'audit délibère régulièrement sur[8]:

- le suivi du processus d'élaboration de l'information financière,
- l'état du contrôle interne et le respect des règles fixées à ce sujet dans la présente circulaire sur base notamment des rapports de la fonction d'audit interne,
- la qualité du travail réalisé par la fonction d'audit interne et le respect des règles fixées à ce sujet dans la présente circulaire (voir sections 6.2.3. et 6.2.7.3),
- la nomination, la reconduction, la révocation et la rémunération du réviseur d'entreprises agréé,
- la qualité du travail réalisé par le réviseur d'entreprises agréé, son indépendance et objectivité, son respect des règles déontologiques en vigueur dans le domaine d'audit. A ce titre, le comité d'audit analyse et évalue d'une manière critique le plan d'audit, les rapports sur les comptes annuels, les "management letters" ainsi que les comptes rendus analytiques réalisés par le réviseur d'entreprises agréé et assure un examen et suivi de l'indépendance du réviseur d'entreprises agréé ou du cabinet de révision agréé, en particulier pour ce qui concerne la fourniture de services complémentaires à l'établissement,
- le suivi approprié et sans délai indu par la direction autorisée des recommandations de la fonction d'audit interne et du réviseur d'entreprises agréé destinées à améliorer l'organisation et le contrôle interne,
- les actions à prendre en cas de problèmes, déficiences et irrégularités relevés par le service d'audit interne et le réviseur d'entreprises agréé,
- le respect des dispositions légales et statutaires ainsi que des règles CSSF pour l'établissement des comptes annuels individuels et, le cas échéant, consolidés, et sur la pertinence des méthodes comptables adoptées.

44. Il est admissible que le comité d'audit couvre également le volet compliance sans qu'un comité de compliance à part soit constitué. Dans ce cas, le mandat et la composition du comité d'audit reflètent ces nouvelles attributions. En particulier, les personnes associées au comité d'audit en vertu du point 39 incluent le « Chief Compliance Officer » suivant le point 105.

Sous-section 4.1.4.2. Le comité des risques

45. Le comité des risques a pour objet d'assister le conseil d'administration dans sa mission d'évaluation de l'adéquation entre les risques encourus, la capacité de l'établissement à gérer ces risques et les fonds propres et réserves de liquidités internes et réglementaires.

[8] L'annexe 2 des lignes directrices du BCBS en matière d'audit interne du 28 juin 2012 (« The internal audit function in banks ») contient une liste plus exhaustive de tâches généralement assignées au comité d'audit.

46. La CSSF recommande aux grands établissements de même qu'aux établissements présentant un profil de risque plus élevé ou complexe de créer un comité des risques afin de faciliter le contrôle effectif des risques par le conseil d'administration.

47. Le comité des risques peut associer à ses travaux la direction autorisée ainsi que les responsables des fonctions de contrôle interne. Ces personnes peuvent assister aux réunions du comité ; elles n'en sont pas membres.

48. Le comité des risques confirme les politiques spécifiques de la direction autorisée suivant la section 4.2.3.

49. Le comité des risques apprécie si les moyens humains et matériels, ainsi que l'organisation de la fonction de contrôle des risques (section 6.2.5.) sont suffisants et s'assure que les membres de la fonction de contrôle des risques possèdent les compétences nécessaires.

50. Le comité des risques délibère régulièrement sur:

- l'état de la gestion des risques et le respect des règles prudentielles fixées à ce sujet,
- la qualité du travail réalisé par la fonction de contrôle des risques et le respect des règles fixées à ce sujet dans la présente circulaire (voir sous-chapitre 6.2.3 et section 6.2.5 en particulier),
- la situation des risques, son évolution future et son adéquation avec la stratégie de l'établissement en matière de risques,
- l'adéquation entre les risques encourus, la capacité actuelle et future de l'établissement à gérer ces risques et les fonds propres et réserves de liquidités internes et réglementaires, eu égard aux résultats de tests d'endurance suivant la circulaire CSSF 11/506,
- le suivi approprié et sans délai indu par la direction autorisée des recommandations de la fonction de contrôle des risques,
- les actions à prendre en cas de problèmes, déficiences et irrégularités relevés par la fonction de contrôle des risques.

51. Le comité des risques conseille le conseil d'administration en matière de définition de la stratégie globale de l'établissement en matière de risques, y compris sa tolérance aux risques actuels et futurs.

Sous-chapitre 4.2. La direction autorisée

Section 4.2.1. Responsabilités de la direction autorisée

52. La direction autorisée est responsable pour la gestion journalière efficace, saine et prudente des activités (et des risques qui leur sont inhérents). Cette gestion s'exerce dans le respect des stratégies et principes directeurs fixés par le conseil d'administration et de la réglementation existante, en prenant en considération et en préservant les intérêts financiers de l'établissement à long terme, sa solvabilité et sa situation des liquidités. Les décisions prises par la direction autorisée dans ces domaines sont dûment documentées.

53. Conformément aux articles 7 paragraphe 2 et 19 paragraphe 2 de la LSF, les membres de la direction autorisée doivent être habilités à déterminer effectivement

l'orientation de l'activité. Par conséquent, lorsque des décisions de gestion sont prises par des comités de gestion plus larges que la seule direction autorisée, il est requis que la direction autorisée en fasse partie et qu'il existe un droit de veto à leur bénéfice.

La direction autorisée doit en principe se trouver de façon permanente sur place. Toute dérogation à ce principe doit être autorisée par la CSSF.

54. La direction autorisée met en œuvre à travers des politiques et procédures internes écrites l'ensemble des stratégies et principes directeurs arrêtés par le conseil d'administration en matière d'administration centrale et de gouvernance interne, dans le respect des dispositions légales et réglementaires et après avoir entendu les fonctions de contrôle interne. Les politiques contiennent les mesures détaillées à mettre en œuvre, les procédures sont les instructions de travail qui régissent cette mise en œuvre. Le terme « procédures » est à prendre au sens large, comprenant l'ensemble des mesures, instructions et règles qui régissent l'organisation et le fonctionnement interne.

    Elle veille à ce que l'établissement dispose de mécanismes de contrôle interne, des infrastructures techniques et des ressources humaines nécessaires pour assurer la gestion saine et prudente des activités (et des risques qui leur sont inhérents) dans le cadre d'un solide dispositif de gouvernance interne conformément à la présente circulaire.

55. En application du point 18 la direction autorisée définit un code de conduite interne applicable à toutes les personnes travaillant dans l'établissement. Elle veille à son application correcte sur base de contrôles réguliers effectués par les fonctions compliance et d'audit interne.

56. La direction autorisée doit avoir une compréhension parfaite de la structure organisationnelle et opérationnelle de l'établissement, en particulier en termes des entités (structures) juridiques sous-jacentes, de leur raison d'être, des liens et interactions intra-groupe qui les relient ainsi que des risques y liés. Elle veille à ce que les informations de gestion requises soient disponibles en temps utile à tous les niveaux de prise de décision et de contrôle de l'établissement et des structures juridiques qui le composent.

57. Dans sa gestion journalière, la direction autorisée tient compte des conseils et avis formulés par les fonctions de contrôle interne.

    Lorsque les décisions prises par la direction autorisée ont ou pourraient avoir une incidence matérielle sur le profil de risque de l'établissement, la direction autorisée recueille au préalable l'avis de la fonction de contrôle des risques et le cas échéant de la fonction compliance.

    La direction autorisée met en œuvre de manière prompte et efficace les mesures correctrices pour remédier aux faiblesses (problèmes, déficiences et irrégularités) relevées par les fonctions de contrôle interne et le réviseur d'entreprises agréé en prenant en compte leurs recommandations en la matière. Cette manière de procéder est arrêtée dans une procédure écrite que le conseil d'administration approuve sur proposition des fonctions de contrôle interne. Suivant cette procédure, les fonctions de contrôle interne classent les différentes faiblesses qu'elles ont identifiées par priorité et fixent, après accord de la direction autorisée, les délais (rapprochés) dans lesquels ces faiblesses sont corrigées. La direction autorisée désigne les unités

opérationnelles ou personnes responsables pour la mise en œuvre des mesures correctrices en leur allouant les ressources (budgets, ressources humaines et infrastructure technique) nécessaires à cet effet. Il appartient aux fonctions de contrôle interne de suivre la mise en application des mesures correctrices. Pour tout retard significatif dans l'implémentation des mesures correctrices, la direction autorisée en informe le conseil d'administration qui doit autoriser les prorogations de délais d'implémentation de mesures correctrices.

L'établissement met en place une procédure analogue, approuvée par le conseil d'administration, qui s'applique lorsque la CSSF demande à l'établissement de prendre des mesures (correctrices). Dans ce cas, tout retard significatif dans l'implémentation de ces mesures est à signaler par la direction autorisée au conseil d'administration et à la CSSF. Cette dernière autorise les prorogations de délais d'implémentation.

58. La direction autorisée vérifie la mise en application et le respect des politiques et procédures internes. Toute violation des politiques et procédures internes doit entraîner des mesures correctrices promptes et adaptées.

59. La direction autorisée s'assure régulièrement de la solidité du dispositif en matière d'administration centrale et de gouvernance interne. Elle adapte les politiques et procédures internes au regard des changements internes et externes, actuels et anticipés, et des enseignements tirés du passé.

60. La direction autorisée informe les fonctions de contrôle interne des changements majeurs en matière d'activités (voir sous-chapitre 7.3) ou d'organisation afin de leur permettre de détecter et d'évaluer les risques qui peuvent en résulter.

61. La direction autorisée informe, de manière complète et par écrit, régulièrement et au moins une fois par an, le conseil d'administration sur l'implémentation, l'adéquation, l'efficacité et le respect du dispositif de gouvernance interne, comprenant l'état de la compliance et celui du contrôle interne, ainsi que le rapport ICAAP[9] sur la situation et la gestion des risques, des fonds propres et des (réserves de) liquidités réglementaires et internes. Ces informations portent en particulier sur l'état du contrôle interne. Une fois par an, la direction autorisée confirme à la CSSF le respect de la présente circulaire par le biais d'une phrase écrite unique suivie des signatures de toute la direction autorisée. Lorsqu'en raison d'un manque de conformité, la direction autorisée n'est pas en mesure de confirmer le respect intégral de la circulaire, la déclaration précitée prend la forme d'une réserve qui énonce sommairement les points de non-conformité en donnant des explications sur leurs raisons d'être.

    Pour les établissements de crédit, les informations à fournir à la CSSF en vertu du premier paragraphe doivent être soumises à la CSSF ensemble avec les comptes annuels à publier.

62. Lorsque la direction autorisée prend connaissance que le dispositif en matière d'administration centrale et de gouvernance interne ne permet plus une gestion saine et prudente des activités ou que les risques encourus ne sont ou ne seront plus adéquatement supportés par la capacité de l'établissement à gérer ces risques, par des fonds propres ou des réserves de liquidités réglementaires ou internes, elle en

[9] Voir le point 26 de la circulaire CSSF 07/301

informe le conseil d'administration et la CSSF en leur fournissant sans délai toute l'information nécessaire pour apprécier la situation (voir également le point 22).

63. Nonobstant la responsabilité collective des membres de la direction autorisée (voir le point 72), cette dernière désigne au moins un de ses membres qui est en charge de l'organisation administrative, comptable et informatique et qui assume la responsabilité de la mise en œuvre de la politique et des règles qu'elle a fixées dans ce domaine. Il est responsable en particulier de l'établissement de l'organigramme et de la description des tâches (voir le point 68) qu'il soumet, avant leur mise en application, à l'approbation de la direction autorisée. Il veille ensuite à leur application correcte. Le membre en question est aussi responsable de la production et de la publication des informations comptables destinées aux tiers et de la communication des informations périodiques à la CSSF. Il veillera donc à ce que la forme et le contenu de ces informations soient conformes aux prescriptions légales et de la CSSF en la matière.

    La direction autorisée désigne également parmi ses membres la ou les personnes en charge des fonctions de contrôle interne.

64. Les établissements informent la CSSF sur les personnes visées au point 105. La direction autorisée rapporte à la CSSF, par écrit et dans les meilleurs délais, les nominations et révocations de ces personnes en communiquant par ailleurs les motifs expliquant la révocation.

Section 4.2.2. Qualification de la direction autorisée

65. Les membres de la direction autorisée possèdent, à la fois individuellement et collectivement, les compétences professionnelles (connaissances, compréhension et expérience), l'honorabilité et les qualités personnelles nécessaires pour gérer l'établissement et déterminer effectivement l'orientation de son activité. Les qualités personnelles sont celles qui leur permettent d'exécuter leur mandat de directeur autorisé de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance requis.

Section 4.2.3. Politiques spécifiques (de risque, de fonds propres et de liquidités)

66. La politique de risque, qui met en œuvre la stratégie du conseil d'administration en matière de risques, comprend:

    - la détermination de la tolérance de l'établissement à l'égard des risques;
    - la définition d'un système complet et cohérent de limites internes qui est adapté à la structure organisationnelle et opérationnelle, aux stratégies et aux politiques de l'établissement et qui limite la prise de risques conformément à la tolérance de l'établissement à l'égard du risque. Ce système inclut les politiques d'acceptation de risques qui définissent quels risques peuvent être pris et quels sont les critères et conditions qui s'appliquent en la matière;
    - les mesures visant à promouvoir une saine culture du risque conformément au point 11;
    - les mesures à mettre en œuvre en vue de garantir une prise et une gestion des risques conformes aux politiques et limites établies. Ces mesures incluent en particulier l'existence d'une fonction de contrôle des risques et d'un dispositif de gestion des dépassements de limites, comprenant une procédure

de régularisation des dépassements, de suivi de la régularisation ainsi que d'escalade et de sanction en cas de dépassement persistant;

- la définition d'un système d'information de gestion en matière de risques;
- les mesures à prendre en cas de matérialisation de risques (dispositif de gestion de crises et de gestion de continuité des activités).

Conformément aux dispositions dans la partie III, chapitre 2, de la présente circulaire la politique de risques tient dûment compte des risques de concentration.

67. La politique en matière de fonds propres et de liquidités, qui met en œuvre la stratégie du conseil d'administration en matière de fonds propres et de liquidités réglementaires et internes, comprend en particulier:

    - la définition de normes internes en matière de gestion, d'ampleur et de qualité des fonds propres et des liquidités réglementaires et internes. Ces normes internes doivent permettre à l'établissement de couvrir les risques encourus et de disposer de marges de sécurité raisonnables en cas de survenance de pertes financières ou d'impasses de liquidités significatives par référence notamment à la circulaire CSSF 11/506;
    - la mise en œuvre de processus intègres et efficaces pour planifier, suivre, rapporter et modifier le montant, le type et la répartition des fonds propres et des réserves de liquidité réglementaires et internes, en particulier par rapport aux besoins de fonds propres et de liquidités internes au titre de couverture des risques. Ces processus permettent à la direction autorisée et au personnel exécutant de disposer d'une information de gestion intègre, fiable et exhaustive en matière des risques et de leur couverture;
    - les mesures mises en œuvre en vue de garantir une adéquation permanente des fonds propres et des (réserves de) liquidités réglementaires et internes ;
    - les mesures prises en vue de gérer efficacement des situations de crise (inadéquation des fonds propres ou impasse de liquidités réglementaires ou internes);
    - la désignation de fonctions responsables pour la gestion, le fonctionnement et l'amélioration des processus, systèmes de limites, procédures et contrôles internes mentionnés aux tirets précédents.

Chapitre 5. Organisation administrative, comptable et informatique

Sous-chapitre 5.1. L'organigramme et les ressources humaines

68. L'établissement doit disposer sur place de ressources humaines suffisantes en nombre et disposant de compétences professionnelles individuelles et collectives appropriées afin de prendre des décisions dans le cadre des politiques fixées par la direction autorisée et sur base de pouvoirs délégués, et afin d'exécuter les décisions prises dans le respect des procédures et de la réglementation existantes. Ces tâches de décision, d'exécution, comprenant l'initiation, l'enregistrement, le suivi et le contrôle des opérations, et de contrôle interne sont effectuées dans le cadre d'un organigramme des fonctions et d'une description des tâches arrêtés par la direction autorisée sous forme écrite. L'organigramme et la description des tâches sont mis à

la disposition de l'ensemble du personnel concerné sous une forme facilement accessible.

69. L'organigramme retient pour les différentes fonctions (commerciales, de support et de contrôle) ainsi que pour les différentes unités opérationnelles (services, départements ou métiers) leur structure et les liens hiérarchiques et fonctionnels entre elles et avec la direction autorisée et le conseil d'administration.

70. La description des tâches à remplir par le personnel exécutant explique la fonction, les pouvoirs et la responsabilité de chaque exécutant.

71. Sans préjudice du point 72, l'organigramme et la description des tâches sont établis sur base du principe de la séparation des tâches. En vertu de ce principe, les tâches et responsabilités doivent être attribuées de façon à éviter qu'elles ne soient incompatibles dans le chef d'une même personne. Le but poursuivi est d'écarter les conflits d'intérêts et de prévenir au moyen d'un environnement de contrôles réciproques qu'une personne puisse commettre des erreurs et irrégularités qui ne seraient pas découvertes.

72. Conformément aux articles 7 paragraphe 2 et 19 paragraphe 2 de la LSF, la direction autorisée a une responsabilité collective en ce qui concerne la gestion de l'établissement. Le principe de la séparation des tâches ne peut pas déroger à cette responsabilité conjointe. Cette dernière reste d'ailleurs compatible avec la pratique suivant laquelle les membres de la direction autorisée se répartissent les tâches journalières du suivi rapproché des différentes activités. Dans ce contexte, la CSSF recommande d'organiser cette répartition de manière à éviter les conflits d'intérêts. Ainsi, il est recommandé de ne pas attribuer à un même membre de la direction autorisée les fonctions de prise de risque et de contrôle indépendant de ces mêmes risques. De même, le directeur autorisé, qui assume lui-même le poste de « Chief Compliance Officer » suivant le point 141, ne peut pas en même temps être en charge de la fonction d'audit interne. Lorsque, en raison de la taille réduite de l'établissement, il est indispensable de regrouper plusieurs tâches et responsabilités sous une même personne, ce regroupement doit être organisé de sorte à ne pas porter préjudice à l'objectif poursuivi par la séparation des tâches.

73. L'établissement dispose d'un programme de formation professionnelle continue qui assure que les membres du personnel ainsi que le conseil d'administration et la direction autorisée restent compétents et comprennent le dispositif de gouvernance interne ainsi que leurs propres rôles et responsabilités à cet égard.

74. Chaque employé doit prendre annuellement au moins dix jours consécutifs de congés personnels. Il doit être assuré que l'employé soit effectivement absent pendant ce congé et que son remplaçant prenne effectivement en charge le travail de la personne absente.

Sous-chapitre 5.2. L'infrastructure administrative et technique

75. L'établissement se dote des fonctions de support, des moyens matériels et techniques nécessaires et suffisants à l'exécution de ses activités. A cet égard, les principes formulés aux sections 5.2.1 à 5.2.5 sont d'application.

Section 5.2.1. L'infrastructure administrative des fonctions commerciales

76. Chaque fonction commerciale doit reposer sur une infrastructure administrative qui garantit la mise en œuvre des décisions commerciales prises et leur bonne exécution, ainsi que le respect des pouvoirs et des procédures pour le domaine en question.

Section 5.2.2. La fonction financière et comptable

77. L'établissement dispose d'un service comptable et financier dont la mission est d'assumer la gestion comptable de l'établissement. Il est permis qu'à l'intérieur de l'établissement certaines parties de la fonction financière et comptable soient décentralisées sous condition toutefois que le service comptable et financier central centralise et contrôle l'ensemble des écritures passées dans les différents services et établisse les comptes globaux. Le service comptable et financier doit veiller à ce que l'intervention d'autres services se fasse dans le strict respect du plan comptable et des instructions y relatives. Le service central reste responsable de la préparation des comptes annuels et de la préparation des informations à fournir à la CSSF.

78. La fonction financière et comptable opère sur base de procédures écrites qui prévoient:

- d'identifier et d'enregistrer toutes les transactions entreprises par l'établissement,
- d'expliquer l'évolution des soldes comptables d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables,
- d'établir les comptes par application des règles de comptabilisation et d'évaluation définies par la législation comptable et la réglementation y afférente,
- de s’assurer de la fiabilité et de la pertinence des prix de marché et justes valeurs (« fair values ») utilisés dans l’établissement des comptes et du reporting à la CSSF,
- de produire et de communiquer des informations périodiques à la CSSF, comprenant en premier lieu le reporting légal et réglementaire, et d’en assurer la fiabilité, notamment en matière de solvabilité, de liquidité et de grands risques.
- de conserver toutes les pièces comptables suivant les dispositions légales en vigueur,
- d'établir, le cas échéant, des comptes suivant le schéma comptable en vigueur dans le pays d'origine de l'actionnaire en vue de l'établissement des comptes consolidés,
- de réaliser les réconciliations des comptes et des écritures comptables ;
- de produire une information de gestion correcte, complète, pertinente, compréhensible et disponible sans délais qui permet à la direction autorisée de suivre de près l'évolution de la situation financière de l'établissement et sa conformité aux données budgétaires. Cette information servira comme instrument de contrôle de gestion et sera d'autant plus efficace si elle est basée sur une comptabilité analytique,
- de s’assurer de la fiabilité du reporting financier.

79. Les établissements se dotent d'un contrôle de gestion qui est soit rattaché au service comptable et financier, soit rattaché dans l'organigramme directement à la direction autorisée de l'établissement.

80. Les tâches exercées au sein du service comptable et financier ne peuvent pas être cumulées avec d'autres tâches incompatibles, tant commerciales qu'administratives.

81. Dans le cadre de l'ouverture de comptes de tiers (bilan et hors-bilan), chaque établissement définit des règles précises d'enregistrement des comptes dans sa comptabilité. Il précise par ailleurs les conditions d'ouverture, de clôture et de fonctionnement de ces comptes.

L'établissement doit éviter d'avoir dans la comptabilité une multitude de comptes avec des contenus incontrôlables, qui se prêteraient à exécuter des opérations non autorisées voire frauduleuses; une attention particulière devra être accordée aux comptes dormants. A cet effet, l'établissement mettra en place des procédures de vérification et de suivi appropriées.

82. L'ouverture et la clôture des comptes internes dans la comptabilité doit être validée par le service comptable et financier. En cas d'ouverture de comptes, cette validation doit intervenir avant que ces comptes ne commencent à devenir opérationnels. L'établissement fixe des règles concernant l'utilisation de pareils comptes et les pouvoirs pour leur ouverture et leur clôture. Le service comptable et financier veille à ce que les comptes internes soient soumis périodiquement à une procédure de justification.

    Il y a lieu de veiller à ne pas tenir ouverts des comptes internes et des comptes de passage qui ne répondraient plus à une utilisation définie par les règles fixées.

83. Les écritures ayant un effet rétroactif ne peuvent servir qu'à des fins de régularisation.

    Les écritures ayant un effet rétroactif ainsi que les écritures en matière d'extournes sont à autoriser et surveiller à la fois au sein des services qui sont à l'origine de ces écritures et au service comptable et financier.

84. L'ensemble de l'organisation et des procédures comptables sont décrites dans un manuel des procédures comptables.

    Dans la définition et la mise en œuvre de ces procédures, les établissements veillent au respect du principe d'intégrité (point 12) afin d'éviter en particulier que le système comptable ne puisse être utilisé à des fins frauduleuses.

Section 5.2.3. La fonction informatique

85. Les établissements organisent leur fonction informatique de manière à en avoir le contrôle et à en assurer la robustesse, l'efficacité, la cohérence et l'intégrité conformément au point 12.

    Ces exigences sont le mieux remplies lorsque la fonction informatique de l'établissement est prise en charge par son propre service informatique organisé et encadré par un dispositif de contrôle interne fixé par la direction autorisée. En règle générale, l'établissement disposera, dans des locaux à sa disposition au Luxembourg de son propre système informatique approprié et dûment documenté et engagera un personnel compétent pour gérer son système informatique.

L’établissement doit être en mesure de fonctionner normalement en cas d’indisponibilité de son système informatique et il dispose à cet effet d’une solution de « back-up » en adéquation avec un plan de continuité et de rétablissement des activités.

86. Les établissements nomment un membre du personnel qui est responsable pour la fonction informatique. Cette personne est désignée par « IT Officer ». Pour des établissements de taille réduite, cette responsabilité peut être assumée par un membre de la direction autorisée qui peut s’appuyer sur une expertise externe.

    Par ailleurs, les établissements nomment un membre du personnel qui est responsable pour la sécurité des systèmes d’informations. Pour des établissements de taille réduite, cette responsabilité peut être assumée par un membre de la direction autorisée qui peut s’appuyer sur une expertise externe. Ce responsable est désigné par « Information Security Officer » ou « Responsable de la Sécurité des Systèmes d’Informations (RSSI) ». Le RSSI est la personne chargée de l’organisation et du pilotage de la sécurité de l’information, c’est-à-dire de la protection de l’information. Il doit être indépendant des fonctions opérationnelles et, selon son positionnement et la taille de l’organisme, dégagé de la mise en œuvre opérationnelle des actions de sécurité. Un mécanisme d’escalade doit lui permettre de rapporter tout problème exceptionnel au plus haut de la hiérarchie, y inclus le conseil d’administration. Ses missions essentielles sont la gestion de l’analyse des risques liés à l’information, la définition des moyens organisationnels, techniques, juridiques et humains requis, le contrôle de leur mise en place et de leur efficacité ainsi que, la conception du/des plan(s) d’actions visant à l’amélioration de la couverture des risques.

    Pour des établissements de taille réduite, un membre unique de la direction autorisée peut assumer les responsabilités de « IT Officer » et de RSSI. Il peut s’appuyer sur une expertise externe.

87. Les établissements qui, en matière de fonction informatique, recourent aux services de tiers respectent en particulier les conditions définies à la section 7.4.2.

Section 5.2.4. Le dispositif de communication et d’alerte internes

88. Le dispositif de communication interne assure que les stratégies, politiques et procédures de l’établissement ainsi que les décisions et mesures prises par le conseil d’administration et la direction autorisée, directement ou par voie de délégation, sont communiquées de manière claire et exhaustive à tous les membres du personnel de l’établissement en tenant compte de leurs besoins d'information et de leurs responsabilités au sein de l'établissement. Le dispositif de communication interne permet au personnel un accès aisé et permanent à ces informations.

89. Le système d’information de gestion assure que toute l’information de gestion, en temps normal et en situation de crise, est communiquée de manière claire, exhaustive et sans délais à tous les membres du conseil d’administration, de la direction autorisée et du personnel de l’établissement en tenant compte de leurs besoins d'information, de leurs responsabilités au sein de l'établissement et de l’objectif d’assurer une gestion saine et prudente des activités.

90. Les établissements maintiennent un dispositif interne d'alerte (« whistleblowing ») qui permet à l’ensemble du personnel de l’établissement d’attirer l'attention sur des préoccupations importantes et légitimes liées à la gouvernance interne. Ce dispositif

respecte la confidentialité des personnes qui soulèvent de telles préoccupations et prévoit la possibilité de soulever ces préoccupations en dehors des lignes hiérarchiques établies ainsi qu'au niveau du conseil d'administration. Les alertes données de bonne foi n'entraînent aucune responsabilité d'aucune sorte dans le chef des personnes qui les ont données.

Section 5.2.5. Le dispositif de gestion de crises

91. Le dispositif de gestion de crises repose sur des ressources (ressources humaines, infrastructure administrative et technique et documentation) qui doivent être aisément accessibles et disponibles en cas d'urgence.

92. Le dispositif de gestion de crises garantit qu'en situation de crise, les établissements de crédit fournissent au public les informations visées par les lignes directrices de l'EBA publiées le 26 avril 2010 (« Principles for disclosures in times of stress (Lessons learnt from the financial crisis) ». Ce point ne s'applique pas aux entreprises d'investissement.

93. Le dispositif de gestion de crises fait l'objet de tests réguliers et de mises à jour en vue d'assurer et de maintenir son efficacité.

Sous-chapitre 5.3. La documentation interne

94. Les établissements documentent par écrit l'ensemble du dispositif en matière d'administration centrale et de gouvernance interne.

    Cette documentation porte sur les stratégies, les principes directeurs, les politiques et les procédures relatifs à l'administration centrale et à la gouvernance interne. Elle comprend en particulier un manuel des procédures clair, complet et facilement accessible au personnel de l'établissement.

95. La description des procédures pour l'exécution des activités (opérations) porte sur les points suivants:

    - étapes successives et logiques du traitement des opérations, de leur initiation à l'archivage de leur documentation,
    - flux des documents utilisés,
    - contrôles périodiques à réaliser, ainsi que moyens pour s'assurer que ceux-ci ont été réalisés.

    Comme le but est de garantir que les opérations sont exécutées de manière correcte, les procédures doivent être claires, mises à jour, complètes dans leur contenu et être connues par tous les employés concernés.

96. Les établissements documentent par écrit l'ensemble de leurs opérations, c'est-à-dire tout processus qui crée un engagement dans le chef de l'établissement ainsi que les décisions y relatives. La documentation doit être tenue à jour et conservée par l'établissement conformément à la loi. Elle doit être organisée de telle manière qu'elle puisse être aisément consultée par un tiers autorisé.

    A titre d'illustration en ce qui concerne les opérations de crédit, une documentation complète des décisions d'accorder, de modifier ou de résilier les crédits se trouve dans les dossiers de l'établissement au Luxembourg, de même que les contrats et toutes pièces relatives au suivi du service de la dette et de l'évolution financière du débiteur.

97. Les dossiers, documents de travail et rapports de contrôle des fonctions de contrôle interne, des experts et des sous-traitants visés au sous-chapitre 6.2 ainsi que les rapports de révision établis par le réviseur d'entreprises agréé sont conservés pendant cinq ans dans l'établissement luxembourgeois afin de permettre à l'établissement de retracer les contrôles effectués, les problèmes, déficiences ou irrégularités relevés ainsi que les recommandations et conclusions. La CSSF ainsi que le réviseur d'entreprises agréé doivent toujours pouvoir accéder à ces pièces.

98. Tous les ordres d'opérations initiées par l'établissement et toute la correspondance avec les clients ou leurs mandataires émanent de l'établissement; toute la correspondance y est adressée. Au cas où l'établissement dispose d'une succursale à l'étranger, cette dernière constitue le point de contact pour sa propre clientèle.

Chapitre 6. Le contrôle interne

99. Le contrôle interne est un dispositif composé de règles et de procédures qui ont pour but d'assurer que les objectifs posés par l'établissement sont atteints, les ressources sont utilisées de façon économique et efficiente, les risques sont contrôlés et le patrimoine est protégé, l'information financière et l'information de gestion sont correctes, complètes, pertinentes, compréhensibles et disponibles sans délais, les lois et réglementations ainsi que les politiques et les procédures internes sont respectées, les demandes et exigences de la CSSF sont respectées.[10]

100. Un environnement de contrôle interne solide nécessite la mise en place des contrôles suivants:

- les contrôles quotidiens réalisés par le personnel exécutant tels que précisés à la section 6.1.1;
- les contrôles critiques continus assurés par le personnel chargé du traitement administratif des opérations tels que précisés à la section 6.1.2;
- les contrôles réalisés par les membres de la direction autorisée sur les activités ou fonctions qui tombent sous leur responsabilité directe tels que précisés à la section 6.1.3;
- les contrôles réalisés par les fonctions de contrôle interne telles que définies au sous-chapitre 6.2.

[10] Les mécanismes de contrôle interne prévoient ainsi des mécanismes destinés à prévenir les erreurs d'exécution et les fraudes et à permettre leur détection rapide. Conformément au principe de proportionnalité, les établissements, dont l'activité de gestion patrimoniale et les activités de services liées notamment à l'administration des OPC sont importantes, définissent des mécanismes de contrôle interne adéquats pour ces activités, notamment pour les domaines de la gestion discrétionnaire, du traitement du courrier domicilié, de la conservation de valeurs de tiers (banque dépositaire), de tenue de comptabilité et de calcul de la valeur nette d'inventaire de fonds d'investissement.

Sous-chapitre 6.1. Les contrôles opérationnels

Section 6.1.1. Contrôles quotidiens réalisés par le personnel exécutant

101. Les procédures en matière de contrôle interne prévoient que les exécutants contrôlent sur une base quotidienne les opérations qu'ils exécutent, ceci afin de détecter le plus rapidement possible des erreurs et omissions survenues dans le traitement des transactions courantes. On peut citer à titre d'exemples de tels contrôles, la vérification du solde de la caisse, la vérification de ses positions par le trader, le suivi de ses suspens par chaque employé.

Section 6.1.2. Contrôles critiques continus

102. Dans cette catégorie de contrôle tombent notamment:

- le contrôle hiérarchique,
- la validation (par exemple la double signature, les codes d'accès à des fonctionnalités données) associée au contrôle du respect de la procédure d'autorisation et de délégation de pouvoirs arrêtée par la direction autorisée (notamment en matière de crédits),
- les contrôles réciproques,
- le relevé régulier de l'existence et de la valeur des éléments du patrimoine, notamment au moyen de la vérification des inventaires,
- la réconciliation et la confirmation des comptes,
- le contrôle de l'exactitude et de l'exhaustivité des données communiquées par les personnes en charge des fonctions commerciales et opérationnelles en vue d'un suivi administratif des opérations,
- le contrôle du respect des limites internes imposées par la direction autorisée (notamment en matière d'activités de marché et de crédits),
- le caractère normal des opérations conclues notamment quant à leur prix, à leur ampleur, aux garanties éventuelles à recevoir ou à fournir, aux bénéfices générés et aux pertes subies, à l'ampleur des frais de courtage éventuels.

Le bon fonctionnement des contrôles critiques continus n'est garanti que si le principe de la séparation des tâches est respecté.

Section 6.1.3. Contrôles réalisés par les membres de la direction autorisée sur les activités ou fonctions qui tombent sous leur responsabilité directe

103. Les membres de la direction autorisée contrôlent personnellement et de manière régulière les activités et fonctions qui tombent sous leur responsabilité directe. Ces contrôles sont effectués sur base des données qui leur sont remises à cet effet par les fonctions commerciales, de support et de contrôle ou les différentes unités opérationnelles de l'établissement.

Les points à surveiller plus particulièrement par ces personnes sont notamment:

- les risques liés aux activités et fonctions dont ils sont directement responsables,

- le respect des lois et normes applicables à l'établissement, avec une attention particulière pour les normes prudentielles en matière de solvabilité, de liquidité et de la réglementation en matière de grands risques,
- le respect des politiques et procédures arrêtées par la direction autorisée conformément au point 18,
- le respect des budgets établis: examen des réalisations effectives et des écarts,
- le respect des limites (notamment sur base d'"exception reports"),
- les caractéristiques des opérations, notamment leur prix, leur rentabilité individuelle,
- l'évolution de la rentabilité globale d'une activité.

Les membres de la direction autorisée informent régulièrement leurs collègues de la direction autorisée sur l'exercice de leur mission de contrôle.

Sous-chapitre 6.2. Les fonctions de contrôle interne

104. Les politiques mises en œuvre en matière de contrôle des risques, de compliance et d'audit interne conformément au point 18 instaurent trois fonctions de contrôle interne distinctes : d'une part, la fonction de contrôle des risques et la fonction compliance qui relèvent de la deuxième ligne de défense et, d'autre part, la fonction d'audit interne qui relève de la troisième ligne de défense (voir point 9). Ces politiques décrivent par ailleurs les domaines d'intervention relevant directement de chaque fonction de contrôle interne, règlent clairement les responsabilités en matière de domaines d'intervention communs et définissent les objectifs ainsi que l'indépendance, l'objectivité et la permanence des fonctions de contrôle interne.

105. Chaque fonction de contrôle interne est placée sous la responsabilité d'un chef de fonction distinct qui est nommé et révoqué suivant une procédure interne écrite. Lorsque, par application du principe de proportionnalité, un membre unique de la direction autorisée exerce les fonctions compliance et de contrôle des risques, cette personne cumule, par dérogation à ce qui précède, les postes de chef de la fonction compliance et de la fonction de contrôle des risques (voir aussi le point 72). Les nominations et révocations des responsables des fonctions de contrôle interne sont approuvées par le conseil d'administration et rapportées par écrit à la CSSF dans le respect de la procédure prudentielle d'approbation des titulaires de fonctions clé telle que publiée par la CSSF sur son site internet.

Les responsables des trois fonctions de contrôle interne sont responsables vis-à-vis de la direction autorisée et, en dernier ressort, vis-à-vis du conseil d'administration pour l'exécution de leur mandat. A ce titre, ces responsables doivent pouvoir contacter et informer directement et de leur propre initiative le président du conseil d'administration ou, le cas échéant, les membres du comité d'audit.

Les responsables des fonctions de contrôle interne sont désignés par « Chief Risk Officer » pour la fonction de contrôle des risques, « Chief Compliance Officer » pour la fonction compliance et « Chief Internal Auditor » pour la fonction d'audit interne.

Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne

106. Les fonctions de contrôle interne ont pour objectif principal de vérifier le respect de l'ensemble des politiques et procédures internes qui tombent dans leur champ d'attribution, d'en évaluer régulièrement l'adéquation par rapport à la structure organisationnelle et opérationnelle, aux stratégies, aux activités et aux risques de l'établissement ainsi que par rapport aux exigences légales et réglementaires applicables et d'en rendre compte directement à la direction autorisée ainsi qu'au conseil d'administration conformément au point 116. Elles fournissent à la direction autorisée ainsi qu'au conseil d'administration les avis et conseils qu'elles jugent utiles en vue d'améliorer le dispositif d'administration centrale et de gouvernance interne de l'établissement.

107. Les fonctions de contrôle interne répondent dans les meilleurs délais aux demandes d'avis et de conseils émanant de la direction autorisée et du conseil d'administration ou des comités spécialisés le cas échéant. Lorsqu'elles estiment que la gestion efficace, saine ou prudente des activités est compromise, les responsables des fonctions de contrôle interne en informent promptement et de leur propre initiative la direction autorisée et le conseil d'administration ou les comités spécialisés, le cas échéant, suivant les modalités internes applicables.

108. Lorsque l'établissement est tête de groupe, ses fonctions de contrôle interne surveillent et contrôlent les fonctions de contrôle interne du groupe. Les fonctions de contrôle interne de l'établissement veillent à ce que les déficiences, irrégularités et risques relevés à travers l'ensemble du groupe soient rapportés aux directions et conseils d'administration locaux ainsi qu'à la direction autorisée et au conseil d'administration de l'établissement conformément au point 116.

Section 6.2.2. Caractéristiques des fonctions de contrôle interne

109. Les fonctions de contrôle interne sont des fonctions permanentes et indépendantes dotées chacune d'une autorité suffisante. Les responsables de ces fonctions ont le droit d'accès direct au conseil d'administration ou à son président, ou, le cas échéant, aux présidents des comités spécialisés qui en émanent, au réviseur d'entreprises agréé de l'établissement ainsi qu'à la CSSF.

    L'indépendance des fonctions de contrôle interne est incompatible avec une situation dans laquelle:

    - le personnel des fonctions de contrôle interne est chargé de tâches qu'il est appelé à contrôler ou de tâches étrangères à son domaine de contrôle respectif,
    - les fonctions de contrôle interne sont intégrées d'un point de vue organisationnel dans les unités opérationnelles qu'elles contrôlent ou dépendent hiérarchiquement d'elles et
    - la rémunération du personnel des fonctions de contrôle interne est liée à la performance des activités qu'elles contrôlent ou déterminée suivant d'autres critères qui compromettent l'objectivité du travail accompli par les fonctions de contrôle interne.

    L'autorité dont doivent jouir les fonctions de contrôle interne requiert que ces fonctions puissent exercer leurs responsabilités de leur propre initiative, s'exprimer librement et accéder à toutes les données et informations externes et

internes (dans l'ensemble des unités opérationnelles de l'établissement qu'elles contrôlent) qui sont jugées nécessaires pour l'accomplissement de leurs missions.

110. Le personnel des fonctions de contrôle interne ou les tiers (voir point 118) agissant pour compte de ces fonctions doivent effectuer leurs travaux avec objectivité.

Afin de garantir leur objectivité, les personnes relevant de fonctions de contrôle interne possèdent l'indépendance d'esprit et de jugement: ils ne doivent pas subordonner leur propre jugement à celui d'autres personnes dont surtout les personnes contrôlées.

L'objectivité exige aussi que les conflits d'intérêts soient évités.

111. Afin de garantir l'efficacité des fonctions de contrôle interne, ses membres doivent posséder à un niveau individuel et collectif des compétences professionnelles élevées dans le domaine des activités bancaires et financières et des normes applicables. Cette compétence doit être évaluée en tenant compte non seulement de la nature de la mission des collaborateurs, mais également de la complexité et de la diversité des activités exercées par l'établissement en vue de permettre une couverture intégrale des activités et des risques. Cette compétence individuelle doit comporter la capacité de porter des jugements critiques et d'être écouté par les directeurs autorisés de l'établissement.

Les fonctions de contrôle interne maintiennent à jour les connaissances acquises et assurent une formation continue et actualisée à chacun de leurs collaborateurs.

En sus de leur expérience professionnelle élevée, les responsables de fonctions de contrôle interne qui accèdent pour la première fois à une telle position possèdent les connaissances théoriques qui leur permettent d'exercer cette fonction d'une manière efficace.

112. Pour garantir l'exécution des tâches qui leur incombent les fonctions de contrôle interne disposent des ressources humaines, de l'infrastructure et des budgets nécessaires et suffisants, conformément au principe de proportionnalité (point 4). Le budget doit être suffisamment flexible pour tenir compte d'une adaptation des missions des fonctions de contrôle en réponse à des changements du profil de risque de l'établissement. Ces dispositions sont compatibles avec une sous-traitance de la fonction d'audit interne et le recours des fonctions de contrôle interne à des experts externes conformément aux points 117 et 118.

113. Le champ d'intervention des fonctions de contrôle interne couvre l'ensemble de l'établissement, dans le respect de leurs compétences respectives. Il inclut les activités inhabituelles et non transparentes visées à la section 7.1.1.

114. Chaque établissement prend les mesures nécessaires pour assurer que les membres des fonctions de contrôle interne exercent leurs fonctions avec intégrité et discrétion.

Section 6.2.3. Exécution des travaux des fonctions de contrôle interne

115. Les fonctions de contrôle interne documentent les travaux effectués conformément aux responsabilités assignées, notamment afin de permettre de retracer les interventions ainsi que les conclusions retenues.

116. Les fonctions de contrôle interne rapportent par écrit régulièrement et si nécessaire sur base ad hoc à la direction autorisée et, le cas échéant, aux comités spécialisés. Ces rapports portent sur le suivi des recommandations, des problèmes, déficiences et irrégularités relevés par le passé ainsi que sur les nouveaux problèmes, déficiences et irrégularités identifiés. Chaque rapport spécifie les risques y liés ainsi que leur degré de gravité (mesure de l'impact) et propose des mesures correctrices, de même qu'en règle générale une prise de position des personnes concernées.

    Chaque fonction de contrôle interne prépare au moins une fois par an un rapport de synthèse sur ses activités et son fonctionnement. Au titre des activités, chaque rapport de synthèse fournit le relevé des principales recommandations adressées à la direction autorisée, des problèmes (existants ou émergents), déficiences et irrégularités significatifs survenus depuis le dernier rapport, des mesures prises à leur égard ainsi que le relevé des problèmes, déficiences et irrégularités significatifs relevés dans le dernier rapport mais qui n'ont pas encore fait l'objet de mesures correctrices appropriées. Le rapport informe également sur les activités liées aux autres responsabilités de la fonction de contrôle, notamment celles définies aux sections 6.2.5, 6.2.6 et 6.2.7. Enfin, le rapport se prononce sur l'état de leur domaine de contrôle dans son ensemble. S'agissant du fonctionnement, le rapport se prononce en particulier sur la nature et le degré du recours à des experts externes conformément au point 118 ainsi que sur les problèmes éventuels apparus dans ce contexte. Ce rapport est soumis pour approbation au conseil d'administration et aux comités spécialisés le cas échéant ; il est soumis pour information à la direction autorisée.

    Conformément au point 107, en cas de problèmes, déficiences et irrégularités graves, les responsables des fonctions de contrôle interne en informent immédiatement la direction autorisée, le président du conseil d'administration et les présidents des comités spécialisés, le cas échéant. Dans ces cas, la CSSF recommande que les responsables des fonctions de contrôle interne soient entendus par les comités spécialisés en séance privée.

    Les fonctions de contrôle interne vérifient le suivi effectif des recommandations relatives aux problèmes, déficiences et irrégularités qu'elles ont relevées, conformément à la procédure visée au troisième paragraphe du point 57. Elles rapportent de manière régulière à ce sujet à la direction autorisée.

Section 6.2.4. Organisation des fonctions de contrôle interne

117. Une sous-traitance de la fonction compliance et de la fonction de contrôle des risques n'est pas admise. Il est admissible que la fonction d'audit interne soit sous-traitée dans de petits établissements dont le profil de risques est faible et non complexe, moyennant le respect des conditions énoncées au point 118 et à la sous-section 6.2.7.4. Cette sous-traitance n'est en principe pas acceptable dans le cas d'établissements qui ont des agences, des succursales ou des filiales.

118. Les dispositions du point 112 n'excluent pas que les fonctions de contrôle interne aient recours à l'expertise ou aux moyens techniques de tiers pour certains aspects. Ce recours est régi par une procédure interne qui doit permettre en particulier à la direction autorisée et au conseil d'administration d'apprécier les dépendances et les risques qui résultent pour l'établissement d'un recours significatif à ces tiers.

La direction autorisée sélectionne ces tiers (« experts ») sur base d'une analyse d'adéquation entre les besoins de l'établissement et les services et compétences spécifiques offerts par ces tiers. L'expert retenu doit être indépendant du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent.

Le recours à un expert externe se fait sur base d'un mandat écrit. L'expert réalise ses travaux dans le respect des dispositions réglementaires et internes (notamment les chartes d'audit interne et de compliance) qui sont applicables à la fonction de contrôle interne et au domaine de contrôle en question. L'expert doit être placé sous la dépendance du responsable de la fonction de contrôle interne dont relève le domaine contrôlé. Ce responsable supervise les travaux de l'expert.

119. Conformément au point 3, les fonctions de contrôle interne d'un établissement doivent également être mises en place au niveau du groupe, des entités juridiques et des succursales qui le composent. Ces parties constituantes doivent être dotées chacune de leurs propres fonctions de contrôle interne en tenant compte du principe de proportionnalité inscrit au point 4.

120. Dans les succursales de l'établissement, les fonctions de contrôle interne dépendent, d'un point de vue hiérarchique et fonctionnel, des fonctions de contrôle de l'établissement tête de groupe dont elles font partie et auxquelles elles font rapport.

    Pour les filiales, les fonctions de contrôle interne dépendent, d'un point de vue fonctionnel, des fonctions de contrôle de l'établissement tête de groupe dont elles font partie. Les rapports établis conformément aux dispositions de la présente circulaire sont soumis non seulement aux organes de direction et de surveillance locaux, mais également, en synthèse, aux fonctions de contrôle interne de l'établissement tête de groupe qui les analyse et qui fait rapport des points à relever, conformément au point 116.

    Lorsque l'établissement n'est pas entreprise mère au sens du point 3, l'établissement s'efforce d'obtenir une synthèse des rapports des fonctions de contrôle interne des entités juridiques en question et les fait analyser par ses propres fonctions de contrôle interne. Celles-ci font rapport des recommandations majeures, des principaux problèmes, déficiences et irrégularités relevés, des mesures correctrices décidées et du suivi effectif de ces mesures conformément au point 116.

    En vertu du point 4, l'établissement peut renoncer à mettre en place auprès d'entités juridiques ou de succursales du groupe des fonctions de contrôle interne propres. Dans ce cas, l'établissement veille à ce que ses fonctions de contrôle interne procèdent régulièrement à des contrôles, y compris des contrôles sur place, auprès de ces entités.

121. Les principes de la présente circulaire n'excluent pas que, pour des établissements luxembourgeois qui sont succursale ou filiale de professionnels financiers luxembourgeois ou non, disposant de fonctions de contrôle interne au niveau de ces professionnels, les fonctions de contrôle interne soient liées de façon fonctionnelle à celles du professionnel en question.

Section 6.2.5. La fonction de contrôle des risques

Remarques:
1. Le lecteur est prié de se référer aussi aux points 9, 17, 21, 33, 45 à 51, 57, 104 à 121, 147 et 179 qui concernent également la fonction de contrôle des risques.
2. Le terme fonction de *contrôle* des risques est emprunté aux lignes directrices de l'EBA (« EBA Guidelines on Internal Governance (GL 44) ». Cette terminologie n'entend pas réduire cette fonction à un simple « contrôle » ex-post de limites en risque tel que visé à la deuxième phrase du point 124. La fonction de contrôle des risques assume plus largement des tâches d'analyse et de suivi des risques conformément au point 123.
3. La fonction de contrôle des risques soumet son rapport annuel de synthèse en copie à la CSSF (points 116 et 210). Conformément au point 116, ce rapport contient un état des lieux en matière de risques et fait ainsi double emploi potentiel avec le rapport ICAAP (point 61) que la direction autorisée prépare à l'attention du conseil d'administration. Le risque de redondances existe d'autant plus que généralement la fonction de contrôle des risques est associée à la rédaction du rapport ICAAP. Afin d'éviter tout double emploi indu entre le rapport ICAAP et le rapport de synthèse de la fonction de contrôle des risques, il suffit que pour l'évaluation du risque suivant l'optique de l'ICAAP, la fonction de contrôle des risques réfère dans son rapport de synthèse au rapport ICAAP pour autant qu'elle partage les descriptifs et analyses de risques qui y figurent. Lorsqu'elle procède de la sorte, la fonction de contrôle des risques doit néanmoins émettre dans son rapport de synthèse ses propres conclusions qu'elle tire des descriptifs et analyses précitées. Le rapport de synthèse porte alors uniquement sur les autres domaines visés au point 116. Par contre, lorsque la fonction de contrôle des risques ne partage pas les descriptifs et analyses précités, elle en fera mention explicite dans son rapport de synthèse où elle fait figurer ses propres évaluations.
4. Un autre domaine de redondances potentielles existe au niveau du partage des tâches entre la fonction compliance, responsable pour les risques de conformité (point 131), et la fonction de contrôle des risques, responsable pour « l'ensemble des risques » (point 123). Les établissements veillent à ce que l'allocation de ces tâches soit organisée en interne d'une manière efficace et efficiente.

122. La fonction de contrôle des risques est confiée à un service dédié composé d'une ou de plusieurs personnes.

123. La fonction de contrôle des risques est responsable pour l'anticipation, la détection, la mesure, le suivi, le contrôle et la déclaration de l'ensemble des risques auxquels l'établissement est ou pourrait être exposé et ainsi d'assister la direction autorisée dans la maîtrise des risques. Elle veille à ce que les risques soient adéquatement gérés.

    Ces tâches sont à réaliser continuellement et sans délais.

    Le champ d'intervention de la fonction de contrôle des risques comprend également les risques inhérents à la complexité de la structure juridique de l'établissement et aux relations de l'établissement avec des parties liées.

Sous-section 6.2.5.1. Responsabilités spécifiques et champ d'application de la fonction de contrôle des risques

124. La fonction de contrôle des risques veille à ce que les limites réglementaires et internes en matière de risque soient compatibles avec les stratégies, les activités et la structure organisationnelle et opérationnelle de l'établissement. Elle contrôle le respect de ces limites, surveille la bonne application de la procédure d'escalade prévue en cas de dépassement et veille à ce que les dépassements soient régularisés dans les meilleurs délais.

125. La fonction de contrôle des risques veille à ce que la direction autorisée et le conseil d'administration reçoivent une vue complète, objective et pertinente des risques auxquels l'établissement est ou pourrait être exposé. Cette vue comprend en particulier une évaluation de l'adéquation entre ces risques et les fonds propres, les (réserves de) liquidités et la capacité de l'établissement à gérer ces risques, en temps normal et en temps de crise. Cette évaluation se fonde en particulier sur le programme de tests de résistance conformément à la circulaire CSSF 11/506. Elle comprend aussi une appréciation quant à l'adéquation entre les risques encourus et les stratégies fixées par le conseil d'administration, en particulier en matière de tolérance à l'égard du risque.

126. La fonction de contrôle des risques veille à ce que la terminologie, les méthodologies et les moyens techniques utilisés à des fins d'anticipation, de détection, de mesure, de déclaration, de gestion et de contrôle des risques soient cohérents et efficaces.

127. La fonction de contrôle des risques veille à ce que l'appréciation qualitative et quantitative des risques se fonde sur des hypothèses prudentes et sur un éventail de scénarios pertinents, en particulier en ce qui concerne les dépendances entre risques. Les appréciations quantitatives sont à valider par des jugements (d'experts) qualitatifs.

    La fonction de contrôle des risques doit régulièrement confronter ses appréciations ex-ante de risques potentiels avec les risques réalisés ex-post en vue d'améliorer la justesse de ses méthodes d'appréciation (« back-testing »).

128. La fonction de contrôle des risques s'attache à anticiper et reconnaître les risques qui émergent dans un environnement changeant. A ce titre, elle suit également la mise en œuvre des modifications d'activités en vue de garantir que les risques y liés restent contrôlés.

Sous-section 6.2.5.2. Organisation de la fonction de contrôle des risques

129. Lorsque, en vertu du principe de proportionnalité (point 4), la création d'un poste de « Chief Risk Officer » à plein temps n'est pas nécessaire, il est admissible d'en charger une personne à temps partiel.

    Il y a lieu de veiller à ce que les autres tâches exercées par cet employé restent compatibles avec les responsabilités lui incombant en vertu des dispositions de la présente circulaire.

    L'établissement qui veut ne pas créer un poste de « Chief Risk Officer » à plein temps en informe la CSSF en lui fournissant une justification de sa décision.

Il est admissible que le membre de la direction autorisée désigné comme étant directement en charge de la fonction de contrôle des risques assume lui-même le poste de « Chief Risk Officer ».

Section 6.2.6. La fonction compliance

Remarques:
1. Le lecteur est prié de se référer aussi aux points 9, 17, 21, 33, 44, 55, 57, 104 à 121, 147 et 179 qui concernent également la fonction compliance.
2. Un domaine de redondances potentielles existe au niveau du partage des tâches entre la fonction compliance, responsable pour les risques de conformité (point 131), et la fonction de contrôle des risques, responsable pour « l'ensemble des risques » (point 123). Les établissements veillent à ce que l'allocation de ces tâches soit organisée en interne d'une manière efficace et efficiente.

130. La fonction compliance est confiée à un service dédié composé d'une ou de plusieurs personnes.

131. La fonction compliance a pour objectif d'anticiper, de détecter et d'évaluer les risques de compliance d'un établissement ainsi que d'assister la direction autorisée dans la maîtrise de ces risques. Ces derniers peuvent comporter une variété de risques tels que le risque de réputation, le risque légal, le risque de contentieux, le risque de sanctions ainsi que certains aspects du risque opérationnel, ceci en relation avec l'intégralité des activités de l'établissement.

    Cette tâche est à réaliser continuellement et sans délais.

    Les établissements qui fournissent des services d'investissement au sens de la LSF mettent en œuvre une fonction compliance qui respecte les orientations de l'ESMA du 6 juillet 2012 (*« Guidelines on certain aspects of the MiFID compliance function requirements* » (ESMA/2012/388)).

Précision:

La présente circulaire comprend les « orientations générales » contenues dans le document ESMA/2012/388 et les applique à l'ensemble des activités de l'établissement, y compris la fourniture de services d'investissement. Lorsqu'ils mettent en œuvre ces exigences en relation avec des services d'investissement au sens de la LSF, les établissements tiennent compte des « orientations complémentaires » formulées dans le document ESMA/2012/388.

Sous-section 6.2.6.1. La charte de compliance

132. Les modalités de fonctionnement de la fonction compliance en termes d'objectifs, de responsabilités et de pouvoirs sont arrêtées par une charte de compliance élaborée par la fonction compliance et approuvée par la direction autorisée et par le conseil d'administration en dernier ressort.

133. La charte de compliance doit au minimum:

    - définir la position de la fonction compliance dans l'organigramme de l'établissement tout en précisant ses caractéristiques clé (indépendance, objectivité, intégrité, compétences, autorité et suffisance des ressources),

- reconnaître à la fonction compliance le droit d'initiative pour ouvrir des enquêtes portant sur toutes les activités de l'établissement y compris celles de ses succursales et filiales au Luxembourg et à l'étranger et à accéder à tous les documents, pièces, procès-verbaux des organes consultatifs et décisionnels de l'établissement, à voir toutes les personnes travaillant dans l'établissement, dans la mesure requise pour l'exercice de sa mission,
- définir les responsabilités et lignes de reporting du « Chief Compliance Officer »,
- décrire les relations avec les fonctions de contrôle des risques et d'audit interne ainsi que d'éventuels besoins de délégation et/ou de coordination,
- définir les conditions et circonstances applicables lorsqu'il est fait recours à des experts externes,
- établir le droit pour le « Chief Compliance Officer » de contacter directement et de sa propre initiative le président du conseil d'administration ou, le cas échéant, les membres du comité d'audit ou du comité de compliance, ainsi que la CSSF.

Le contenu de la charte de compliance est porté à la connaissance de tous les membres du personnel de l'établissement, y compris ceux qui travaillent dans les succursales à l'étranger et dans les filiales au Luxembourg et à l'étranger.

134. La charte de compliance doit être mise à jour dans les meilleurs délais pour tenir compte de changements au niveau des normes en vigueur affectant l'établissement. Toutes les modifications doivent être approuvées par la direction autorisée, confirmées par le comité d'audit ou le comité de compliance, le cas échéant, et approuvées par le conseil d'administration en dernier ressort. Elles sont portées à la connaissance de tous les membres du personnel.

Sous-section 6.2.6.2. Responsabilités spécifiques et champ d'application de la fonction compliance

135. Pour atteindre les objectifs fixés, les responsabilités de la fonction compliance doivent couvrir au moins les aspects suivants:
    - La fonction compliance identifie les normes auxquelles l'établissement est soumis dans l'exercice de ses activités dans les différents marchés et tient le relevé des règles essentielles. Ce relevé doit être accessible au personnel concerné de l'établissement.
    - La fonction compliance identifie les risques de compliance auxquels l'établissement est exposé dans le cadre de l'exercice de ses activités et en évalue l'importance et les conséquences possibles. Le classement des risques de compliance ainsi déterminé doit permettre à la fonction compliance d'établir son plan de contrôle en fonction du risque, permettant ainsi une utilisation efficace des ressources de la fonction compliance.
    - La fonction compliance veille à l'identification et l'évaluation du risque de compliance avant que l'établissement ne se lance dans un nouveau type d'activité, de produit ou de relation d'affaires, de même que lors du développement des opérations et du réseau d'un groupe sur une échelle internationale.

- La fonction compliance veille à ce que, pour la mise en œuvre de la politique de compliance, l'établissement dispose de règles qui puissent servir de lignes directrices au personnel des différents métiers dans l'exercice de ses tâches journalières. Ces règles doivent être reflétées de façon appropriée dans les instructions, procédures et contrôles internes pour les domaines relevant directement de la compliance. Dans l'élaboration de ces règles, la fonction compliance tient compte, pour autant que de besoin pour l'établissement en question, des règles de déontologie énoncées dans le dispositif de la gouvernance interne.
- Les domaines qui relèvent directement de la fonction compliance sont typiquement la lutte contre le blanchiment et le financement du terrorisme, la prévention en matière d'abus de marché et de transactions personnelles, l'intégrité des marchés d'instruments financiers, la protection des intérêts des clients et des investisseurs, la protection des données et le respect du secret professionnel, la prévention et la gestion des conflits d'intérêts, la prévention de l'utilisation du secteur financier par des tiers pour contourner leurs obligations réglementaires et la gestion du risque de conformité lié aux activités transfrontalières. Dans le cadre plus général du respect du code de conduite, la fonction compliance est aussi amenée à couvrir des domaines d'éthique et de déontologie, voire de fraudes. Cette liste n'est pas exhaustive. D'une manière générale, la fonction compliance est à organiser de telle manière qu'elle couvre tous les domaines pouvant donner lieu à des risques de compliance. Toutefois, dans la mesure où dans la pratique certains domaines donnant lieu à des risques de compliance peuvent aussi relever d'autres fonctions telles que la fonction de contrôle des risques, la fonction finance ou la fonction juridique, et dans un souci d'éviter une duplication des contrôles de compliance, il est admissible que les domaines autres que ceux énumérés ci-dessus ne soient pas directement couverts par la fonction compliance. Il est entendu que dans ce cas, le risque de compliance est alors à couvrir par les autres fonctions de contrôle interne suivant une politique de compliance définissant clairement les attributions et les responsabilités des différents intervenants en la matière et moyennant le respect de la ségrégation des tâches. Dans ce cas, le « Chief Compliance Officer » assume un rôle de coordination, de centralisation et de vérification que les autres domaines ne relevant pas directement de son champ d'intervention sont bien couverts.
- Il appartient à l'établissement de décider si, compte tenu des particularités des activités exercées, sa fonction compliance couvre le contrôle du respect des règles n'ayant pas directement trait aux activités bancaires et financières à proprement parler, telles que notamment les règles relevant du droit de travail, du droit social, du droit des sociétés ou du droit de l'environnement.

136. La fonction compliance procède régulièrement à une vérification du respect de la politique de compliance et des procédures et se charge, en cas de besoin, des propositions d'adaptation. A cette fin la fonction compliance effectue des évaluations et des contrôles réguliers du risque de compliance. Pour les contrôles en matière de risque de compliance ainsi que pour la vérification des procédures et des instructions, les dispositions de la présente circulaire n'empêchent pas que la fonction compliance prenne en compte les travaux de l'audit interne.

137. La fonction compliance centralise toutes les informations sur les problèmes de compliance (entre autres les infractions aux normes, le non-respect de procédures ou encore les conflits d'intérêts) détectés dans l'établissement.

Pour autant qu'elle ne tire pas ces informations de sa propre implication, elle procède à un examen des documents pertinents, qu'ils soient internes (par exemple rapports de contrôle et d'audit interne, rapports ou comptes rendus de la direction autorisée ou, le cas échéant, du conseil d'administration) ou externes (par exemple rapports du réviseur externe, correspondance de la part de l'autorité de contrôle).

138. La fonction compliance assiste et conseille la direction autorisée pour des questions de compliance et de normes, notamment en la rendant attentive à des développements au niveau des normes qui pourraient ultérieurement avoir un impact sur le domaine de la compliance.

139. La fonction compliance veille à sensibiliser le personnel à l'importance de la compliance et des aspects connexes et à l'assister dans ses activités quotidiennes relatives à la compliance. Elle développe à ces fins également un programme de formation continue et s'assure de sa mise en œuvre.

140. Le « Chief Compliance Officer » est la personne de contact privilégié des autorités compétentes en matière de lutte contre le blanchiment et le financement du terrorisme pour toute question relative à ce domaine ainsi qu'en matière d'abus de marché. Il est également en charge de la transmission de toute information ou déclaration auprès desdites autorités.

Sous-section 6.2.6.3. Organisation de la fonction compliance

141. Lorsque, en vertu du principe de proportionnalité (point 4), la création d'un poste de «Chief Compliance Officer» à plein temps n'est pas nécessaire, il est admissible d'en charger une personne à temps partiel.

Il y a lieu de veiller à ce que les autres tâches exercées par cet employé restent compatibles avec les responsabilités lui incombant en vertu des dispositions de la présente circulaire.

L'établissement qui veut ne pas créer un poste de «Chief Compliance Officer» à plein temps, doit obtenir l'autorisation explicite de la CSSF. A cette fin, la direction autorisée et le président du conseil d'administration soumettent à la CSSF une demande écrite fournissant une justification ainsi que les informations nécessaires afin de permettre d'évaluer que l'application correcte des dispositions de la présente circulaire et la bonne exécution de la fonction compliance restent assurées.

Il est admissible, moyennant autorisation spécifique de la CSSF, que le membre de la direction autorisée désigné comme étant directement en charge de la fonction compliance assume lui-même le poste de «Chief Compliance Officer».

Section 6.2.7. La fonction d'audit interne

Remarque:
Le lecteur est prié de se référer aussi aux points 9, 17, 21, 33, 38 à 44, 55, 57 et 104 à 121 qui concernent également la fonction d'audit interne.

142. La fonction d'audit interne est confiée à un service d'audit interne, composé d'une ou de plusieurs personnes.

143. La fonction d'audit constitue à l'intérieur de l'organisation de l'établissement une fonction indépendante et permanente d'évaluation critique de l'adéquation et de l'efficacité de l'administration centrale, de la gouvernance interne et de la gestion des activités et des risques dans leur intégralité afin d'assister le conseil d'administration et la direction autorisée de l'établissement et leur permettre d'avoir la meilleure maîtrise de leurs activités et des risques y liés et ainsi de protéger son organisation et sa réputation.

Sous-section 6.2.7.1. La charte d'audit interne

144. Les modalités de fonctionnement de la fonction d'audit interne en termes d'objectifs, de responsabilités et de pouvoirs doivent être arrêtées par une charte d'audit interne élaborée par la fonction d'audit interne et approuvée par la direction autorisée, confirmée par le comité d'audit, le cas échéant, et approuvée en dernier ressort par le conseil d'administration.

La charte d'audit interne doit au minimum:

- définir la position de la fonction d'audit interne dans l'organigramme de l'établissement tout en en précisant les caractéristiques clé (indépendance, objectivité, intégrité, compétence, autorité, suffisance des ressources),
- conférer à la fonction d'audit interne le droit d'initiative et l'autoriser à examiner toutes les activités et fonctions de l'établissement y compris celles de leurs succursales à l'étranger et filiales au Luxembourg et à l'étranger, à accéder à tous les documents, pièces, procès-verbaux des organes consultatifs et décisionnels de l'établissement, à voir toutes les personnes travaillant dans l'établissement, dans la mesure requise pour l'exercice de sa mission,
- définir les lignes de communication hiérarchiques et fonctionnelles des conclusions qui se dégagent des missions d'audit,
- définir les relations avec les fonctions compliance et de contrôle des risques,
- définir les conditions et circonstances applicables lorsqu'il est fait recours à l'expertise de tiers,
- définir la nature des travaux et les conditions dans lesquelles la fonction d'audit interne peut fournir de la consultance interne ou effectuer d'autres missions spéciales,
- définir les responsabilités et lignes de reporting du responsable de la fonction d'audit interne,
- établir le droit pour le « Chief Internal Auditor » de contacter directement et de sa propre initiative le président du conseil d'administration ou, le cas échéant, les membres du comité d'audit ainsi que la CSSF,

- préciser que les missions d'audit interne sont effectuées en conformité avec des standards professionnels reconnus11,
- préciser les procédures à respecter en matière de coordination et de coopération avec le réviseur d'entreprises agréé.

Le contenu de la charte d'audit interne est porté à la connaissance de tous les membres du personnel de l'établissement, y compris ceux qui travaillent dans les succursales à l'étranger et dans les filiales au Luxembourg et à l'étranger.

La charte d'audit interne doit être mise à jour dans les meilleurs délais pour tenir compte des changements intervenus. Toutes les modifications doivent être approuvées par la direction autorisée, confirmées le cas échéant par le comité d'audit et approuvées par le conseil d'administration en dernier ressort. Elles sont portées à la connaissance de tous les membres du personnel.

145. En complément des points 110 à 112, le service d'audit interne est suffisant en nombre et dispose de compétences suffisantes dans son ensemble pour couvrir toutes les activités de l'établissement. Les auditeurs internes doivent avoir des connaissances suffisantes des techniques d'audit.

Afin de ne pas compromettre leur indépendance de jugement, les personnes relevant de l'audit interne ne peuvent pas être chargées de l'élaboration ou de la mise en place d'éléments du dispositif en matière d'administration centrale et de gouvernance interne. Ce principe n'exclut pas qu'elles contribuent à la mise en œuvre de mécanismes de contrôle interne solides à travers des avis et des recommandations qu'elles fournissent en la matière (voir en particulier le point 107). De plus, en vue d'éviter les conflits d'intérêts, il y a lieu, dans la mesure du possible, d'assurer une rotation des tâches de contrôle assignées aux différents auditeurs internes et d'éviter que les auditeurs recrutés au sein de l'établissement ne contrôlent des activités ou fonctions qu'ils exerçaient eux-mêmes auparavant dans un passé récent.

Sous-section 6.2.7.2. Responsabilités spécifiques et champ d'application de la fonction d'audit interne

146. D'une manière générale, la fonction d'audit interne examine et évalue si le dispositif en matière d'administration centrale et de gouvernance interne est adéquat et fonctionne de manière efficace. A ce titre, la fonction d'audit interne évalue, entre autres :
    - le suivi du respect des lois et réglementations ainsi que des exigences prudentielles imposées par la CSSF,
    - l'efficacité et l'efficience du contrôle interne,
    - l'adéquation de l'organisation administrative, comptable et informatique
    - la sauvegarde des valeurs et des biens,
    - l'adéquation de la séparation des tâches et de l'exécution des opérations,

[11] tel que par exemple le « International Professional Practices Framework (IPPF) » de l'Institute of Internal Auditors (IIA)

- l’enregistrement correct et exhaustif des opérations et la production d’informations financières et prudentielles correctes, complètes, pertinentes, compréhensibles et disponibles sans délais au conseil d’administration et aux comités spécialisés, le cas échéant, à la direction autorisée et à la CSSF,
- l’exécution des décisions prises par la direction autorisée et par les personnes agissant par voie de délégation et sous sa responsabilité,
- le respect des procédures régissant l’adéquation des fonds propres et des réserves de liquidité internes en application des points 67 deuxième et troisième tirets et 125,
- l’adéquation de la gestion des risques,
- le fonctionnement et l’efficacité des fonctions compliance et de contrôle des risques (sections 6.2.5 et 6.2.6).

147. Lorsqu’il existe à l’intérieur de l’établissement un service distinct en charge du contrôle ou de la surveillance d’une activité ou d’une fonction spécifique, l’existence d’un tel service ne décharge pas le service d’audit interne de sa responsabilité de contrôler ce domaine spécifique. Toutefois, le service d’audit interne peut tenir compte dans son travail des appréciations données par ce service sur le domaine en question.

    L’audit interne doit être indépendant des autres fonctions de contrôle interne qu’il audite. Par conséquent, la fonction de contrôle des risques ou la fonction compliance ne peuvent pas faire partie du service d'audit interne d'un établissement. Cependant, ces fonctions peuvent prendre en compte les travaux de l'audit interne en matière de vérification de l'application correcte des normes en vigueur à l'exercice des activités exercées par l'établissement.

148. En complément des points 119 et 120, la mise en place d’une fonction d’audit interne local dans les filiales de l’établissement ne dispense pas l’audit interne de la tête de groupe de procéder régulièrement à des contrôles sur place auprès de ces fonctions d’audit interne locaux.

149. Le « Chief Internal Auditor » doit s’assurer que le service applique les normes internationales de l'lnstitute of Internal Auditors ou des normes internationales équivalentes en application du point 21 ainsi que les règles de conduite en application du point 55.

Sous-section 6.2.7.3. Exécution des travaux d’audit interne

150. L’ensemble des missions d’audit interne est planifié et exécuté selon un «plan d’audit interne». Le plan est établi par le responsable de la fonction d’audit interne pour une période pluriannuelle (en principe trois ans) avec comme objectif de couvrir l’ensemble des activités et des fonctions, en tenant compte à la fois des risques que présentent une activité ou une fonction de l’établissement et de l’efficacité de l’organisation et du contrôle interne en vigueur pour cette activité ou fonction. Le plan tient compte des avis du conseil d’administration et du comité d’audit, le cas échéant, ainsi que de la direction autorisée. Le plan couvre toutes les matières présentant un intérêt prudentiel (y compris les observations et les demandes de la CSSF) et tient compte également des développements et innovations prévus ainsi que des risques qui peuvent en découler.

151. Le plan est discuté avec la direction autorisée et soumis à la direction autorisée et approuvé par elle, confirmé par le comité d'audit, le cas échéant, et approuvé en dernier ressort par le conseil d'administration. Il est à revoir sur une base annuelle et à adapter le cas échéant en fonction des développements et des urgences. Toute adaptation est à approuver formellement par la direction autorisée et le comité d'audit, le cas échéant. L'approbation implique que la direction autorisée mette à la disposition du service d'audit interne les moyens nécessaires pour l'exécution du plan d'audit interne.

    Dans son rapport de synthèse au conseil d'administration suivant le point 116, l'audit interne signale et motive les principales modifications apportées au plan d'audit tel qu'il a été approuvé initialement par le conseil d'administration : missions annulées, missions reportées ainsi que missions dont le champ d'application a été changé de manière significative.

152. Le plan qui est suffisamment documenté, définit les objectifs de chaque mission et l'étendue des travaux à réaliser, estime le temps et les ressources humaines et matérielles nécessaires et attribue à chaque activité et risque une fréquence d'audit.

    Le plan d'audit interne prévoit également de couvrir, endéans la période de planification pluriannuelle, de façon adéquate et suffisamment fréquente les activités importantes ou complexes qui représentent un risque potentiel important, y compris sur le plan de la réputation. Il accorde une attention particulière au risque d'erreurs d'exécution et au risque de fraude.

153. Dans l'hypothèse où le service d'audit interne de la maison mère de l'établissement luxembourgeois procède régulièrement à des contrôles sur place auprès de sa filiale, il se recommande pour des raisons d'efficacité, que l'établissement luxembourgeois coordonne, dans la mesure du possible, son plan d'audit interne avec celui de sa maison mère.

154. Le service d'audit interne informe la direction autorisée et, le cas échéant, le comité d'audit de façon régulière sur l'exécution du plan d'audit interne.

155. Chaque mission d'audit interne est planifiée, exécutée et documentée en conformité avec les standards professionnels adoptés par la fonction d'audit interne dans sa charte d'audit interne.

156. Chaque mission doit faire l'objet d'un rapport écrit du service d'audit interne destiné, en règle générale, aux personnes contrôlées, à la direction autorisée ainsi que - éventuellement sous forme de synthèse - au conseil d'administration (et au comité d'audit, le cas échéant) suivant le point 116. Les rapports sont également à tenir à disposition du réviseur d'entreprises agréé et de la CSSF. Ces rapports sont à rédiger en français, allemand ou anglais.

    Le service d'audit interne établit un tableau des missions d'audit interne et des rapports écrits y relatifs. Il rédige au moins une fois par an un rapport de synthèse conformément au point 116.

Sous-section 6.2.7.4. Organisation de la fonction d'audit interne

157. L'établissement qui conformément au point 117 décide de sous-traiter la fonction d'audit interne, doit introduire une demande écrite auprès de la CSSF. Cette demande comprend les informations nécessaires à son appréciation, dont

notamment le nom de l'expert externe, personne physique, qui assumera la fonction d'audit interne de l'établissement.

Le choix de l'expert externe qui réalise les travaux d'audit interne doit être approuvé par le conseil d'administration, le cas échéant sur base de l'avis du comité d'audit créé par application du point 33. L'expert retenu doit être indépendant du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent. Il réalise ses travaux conformément au point 118 et, mutatis mutandis, aux dispositions contenues dans la présente circulaire. A ce titre, il s'acquitte de l'ensemble des tâches et responsabilités que la présente circulaire donne à l'audit interne.

158. En cas de recours à un expert externe pour certains aspects conformément au point 118, cet expert réalise ses travaux dans le cadre du plan d'audit interne de l'établissement en suivant un programme de travail, en documentant ses travaux de façon détaillée et en rédigeant des rapports pour chaque mission. Ces rapports sont à rédiger en français, allemand ou anglais et sont à remettre au « Chief Internal Auditor », à la direction autorisée, au comité d'audit, le cas échéant, et au conseil d'administration suivant le point 116.

159. Les experts externes suivant le point 118 peuvent être les auditeurs internes du groupe dont fait partie l'établissement. Lorsque les experts exercent la profession de réviseur d'entreprises agréé, ils doivent à tous égards être indépendants du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent.

Chapitre 7. Exigences spécifiques

Sous-chapitre 7.1. Structure organisationnelle et entités juridiques (« Know-your-structure »)

160. La structure organisationnelle, en termes d'entités (structures) juridiques, est appropriée et justifiée par rapport aux stratégies et principes directeurs visés au point 17 de la présente circulaire.

Elle doit permettre et promouvoir une gestion efficace, saine et prudente des activités. Elle ne doit pas entraver la capacité de l'établissement, en particulier de ses organes d'administration et de direction, à gérer et à contrôler efficacement les activités (et les risques) de l'établissement et des différentes entités juridiques qui le composent.

L'établissement tête de groupe délimite et définit de façon explicite les pouvoirs qu'il accepte de déléguer aux dirigeants des entités juridiques qui composent le groupe en vue de s'assurer que la tête de groupe puisse suivre de façon continue leur activité et qu'elle soit impliquée lors de toute opération d'une certaine importance.

161. Les principes directeurs que le conseil d'administration arrête en matière de structure organisationnelle (en termes d'entités juridiques) prévoient en particulier que

- la structure organisationnelle est exempte de toute complexité indue;

- la production et la circulation en temps utile de toutes les informations nécessaires à une gestion saine et prudente de l'établissement et des entités juridiques qui le composent sont garanties;
- tout flux d'information de gestion matérielle entre entités juridiques composant l'établissement est documenté et peut être fourni promptement au conseil d'administration, à la direction autorisée, aux fonctions de contrôle interne ou à la CSSF, à leur demande.

Section 7.1.1. Principes directeurs en matière d'activités « inhabituelles » ou « non transparentes »

162. Les activités « inhabituelles » ou « non transparentes » sont celles qui sont réalisées à travers des entités (structures) juridiques dédiées ou assimilées (« special purpose vehicles ») ou dans des territoires qui accusent des déficits en matière de transparence ou qui ne répondent pas aux normes bancaires internationales.

163. Les principes directeurs que le conseil d'administration arrête en matière de gouvernance interne prévoient en particulier que les activités inhabituelles ou non transparentes

- ne sont acceptables qu'à condition que l'établissement ait l'assurance que les risques inhérents peuvent être gérés efficacement ;
- sont maîtrisées à travers des processus d'approbation et de gestion des risques et des informations de gestion disponibles au niveau de la direction autorisée et des fonctions de contrôle interne de l'établissement ;
- sont sujettes à un contrôle régulier en vue d'assurer qu'elles restent nécessaires et conformes à leurs buts d'origine et
- sont régulièrement contrôlées par les fonctions de contrôle interne et par le réviseur d'entreprises agréé de l'établissement.

164. Les points 162 et 163 s'appliquent aussi lorsque l'établissement mène des activités inhabituelles ou non transparentes pour le compte de ses clients.

Sous-chapitre 7.2. Gestion des conflits d'intérêts

165. La politique en matière de gestion des conflits d'intérêts couvre l'ensemble des conflits d'intérêts, avec une attention particulière pour les conflits d'intérêts entre l'établissement et ses parties liées et parties tierces sous-traitantes. Cette politique est applicable à tout le personnel ainsi qu'à la direction autorisée et les membres du conseil d'administration.

166. La politique en matière de gestion des conflits d'intérêts prévoit que tous les conflits d'intérêts actuels et potentiels doivent être détectés, avec pour objectif de les éviter. Lorsque des conflits d'intérêts subsistent, la politique en la matière fixe les procédures à suivre en vue de les rapporter et de les gérer dans l'intérêt de l'établissement et conformément aux dispositions réglementaires applicables en matière de protection des clients. La politique en question fixe également la procédure à suivre en cas de non respect de la politique en question.

167. La politique en matière de gestion des conflits d'intérêts identifie les principales sources de conflits d'intérêts - les relations et activités potentiellement concernées

ainsi que l'ensemble des parties internes et externes impliquées – auxquels l'établissement est ou pourrait être confronté et arrête la manière dont ces conflits d'intérêts doivent être gérés. Afin de minimiser le potentiel de conflits d'intérêts, l'établissement met en place une ségrégation appropriée des tâches et activités.

168. Lorsqu'ils sont ou ont été confrontés à un conflit d'intérêts, les membres du personnel en informent leur supérieur hiérarchique promptement et de leur propre initiative. Ce dernier, lorsqu'il constate que le conflit d'intérêt est acceptable au vu de la politique interne, l'autorise suivant les modalités et conditions prévues par cette politique. La politique en question fixe également la procédure d'escalade qui détermine les conflits d'intérêts qui doivent être rapportés à la direction autorisée et autorisés par celle-ci.

169. Les membres de la direction autorisée et du conseil d'administration qui sont sujets à un conflit d'intérêts en informent respectivement la direction autorisée ou le conseil d'administration de manière prompte et de leur propre initiative. Les procédures en la matière prévoient que ces membres s'abstiennent de participer aux prises de décision qui leur causent un conflit d'intérêts ou qui les empêchent de décider en toute objectivité et indépendance.[12]

170. La détection et la gestion des conflits d'intérêts appartiennent au champ d'intervention des fonctions de contrôle interne.

Section 7.2.1. Exigences additionnelles relatives aux conflits d'intérêts en relation avec des parties liées

171. Les relations d'affaires avec des parties liées sont soumises pour approbation au conseil d'administration lorsqu'elles ont ou pourraient avoir une influence significative et défavorable sur le profil de risque de l'établissement. La règle s'applique également lorsqu'en l'absence d'effet significatif au niveau de chaque transaction prise individuellement, l'influence est significative pour l'ensemble des transactions avec des parties liées.

172. Tout changement matériel relatif à des transactions significatives effectuées avec des parties liées doit être porté à l'attention du conseil d'administration dans les meilleurs délais.

173. Les transactions avec des parties liées doivent être réalisées dans l'intérêt de l'établissement. L'intérêt de l'établissement n'est pas respecté lorsqu'il s'agit en particulier de transactions avec des parties liées qui

- sont réalisées à des conditions moins avantageuses (dans le chef de l'établissement) que celles qui s'appliqueraient à la même transaction réalisée avec une partie tierce (« at arm's length »);
- ont pour effet de porter atteinte à la solvabilité, à la situation des liquidités ou aux capacités de gestion des risques de l'établissement sur le plan réglementaire ou interne;

[12] Cette disposition rejoint celle de l'article 57 de la loi du 10 août 1915 concernant les sociétés commerciales qui dispose que dans le chef des sociétés anonymes et des sociétés européennes « l'administrateur qui a un intérêt opposé à celui de la société, dans une opération soumise à l'approbation du conseil d'administration, est tenu d'en prévenir le conseil et de faire mentionner cette déclaration au procès-verbal de la séance. Il ne peut prendre part à cette délibération. ».

- dépassent les capacités de gestion et de contrôle des risques de l'établissement;
- sont contraires aux principes d'une gestion saine et prudente dans l'intérêt de l'établissement.

174. Lorsqu'il est tête de groupe, l'établissement veille à prendre en compte d'une manière équilibrée et dans le respect des dispositions légales applicables, les intérêts de toutes les entités juridiques et succursales qui composent le groupe. Ces intérêts sont à apprécier à la lumière de leur contribution aux objectifs et intérêts communs du groupe à long terme.

Sous-chapitre 7.3. Procédure d'approbation des nouveaux produits (et des nouvelles activités) (« New Product Approval Process »)

175. On entend par « nouveaux produits » toute modification de l'activité (en termes de couverture de marchés et de clientèle, de produits et de services).

176. Aucune nouvelle activité ne doit être entreprise avant que l'approbation n'ait été donnée par la direction autorisée, après avoir entendu toutes les parties concernées, et que les moyens mentionnés au point 179 ne soient disponibles. Le processus en question est fixé dans une procédure d'approbation des nouveaux produits qui respecte les dispositions des points 177 à 180.

177. La procédure d'approbation des nouveaux produits définit en particulier les modifications d'activités sujettes à la procédure d'approbation (modification d'activité dite significative) ainsi que le déroulement de la procédure d'approbation, y compris les responsabilités.

178. La procédure d'approbation fixe les droits et obligations de toutes les parties concernées, y compris les fonctions de contrôle interne, ainsi que les conditions à remplir en vue d'une approbation. Ces conditions incluent la compliance, la maîtrise des calculs de valorisation (« pricing ») et des risques, l'expertise interne, l'infrastructure technique et les ressources humaines suffisantes pour assurer l'ensemble du traitement opérationnel.

179. Les établissements analysent avec soin tout projet de modification d'activités et s'assurent qu'ils disposent de la capacité à supporter les risques y liés, de l'infrastructure technique et des ressources humaines suffisantes et compétentes pour maîtriser ces activités et les risques qui leur sont associés. Il appartient à l'unité opérationnelle qui demande la modification de ses activités de produire une analyse des risques en la matière. De même, la fonction de contrôle des risques procède à une analyse préalable, objective et complète des risques liés à tout projet de modification d'activités. L'analyse des risques tient compte de différents scénarios et se prononce en particulier sur la capacité de l'établissement à supporter, à gérer et à contrôler les risques inhérents aux activités projetées. Le risque de compliance inhérent à de nouveaux produits fait l'objet d'une analyse préalable par la fonction compliance. Pour leurs avis, les fonctions de contrôle interne peuvent s'appuyer sur les analyses faites par les unités opérationnelles.

180. Les fonctions de contrôle interne peuvent exiger qu'une modification d'activités soit classée comme significative et soumise par conséquent à la procédure d'approbation.

Sous-chapitre 7.4. Sous-traitance (« Outsourcing »)

181. La sous-traitance désigne le transfert complet ou partiel de tâches opérationnelles, d'activités ou de prestations de services de l'établissement vers un prestataire externe, qui fait partie ou non du groupe auquel l'établissement appartient.

Pour les besoins de ce sous-chapitre, le terme « activité » sert à désigner les tâches opérationnelles, activités et prestations de services visées au premier paragraphe. Est considérée comme « matérielle » toute activité qui, lorsqu'elle n'est pas exécutée dans les règles, diminue la capacité de l'établissement à respecter les exigences réglementaires ou à poursuivre ses opérations, ainsi que toute activité qui est nécessaire à la gestion saine et prudente des risques.

Section 7.4.1. Exigences générales en matière de sous-traitance

182. La sous-traitance ne doit pas aboutir à ce que les règles de la présente circulaire en matière d'administration centrale (chapitres 1 et 3) ne soient plus respectées.

L'établissement qui sous-traite se conforme en particulier aux exigences suivantes :

- Les fonctions stratégiques ou relevant du cœur de métier ne peuvent pas être sous-traitées;
- L'établissement conserve l'expertise nécessaire pour contrôler efficacement les prestations ou les tâches sous-traitées et la gestion des risques associés à la sous-traitance;
- La protection des données doit être garantie en permanence;
- La sous-traitance ne décharge pas l'établissement de ses obligations légales et réglementaires ou de ses responsabilités envers la clientèle. Elle n'entraîne aucune délégation de responsabilité de l'établissement vers le sous-traitant, sauf concernant la responsabilité du secret professionnel lorsque le sous-traitant agit dans le cadre de l'article 41(5) de la LSF;
- La responsabilité finale de la gestion des risques associés à la sous-traitance incombe à la direction autorisée de l'établissement procédant à la sous-traitance;
- L'établissement s'assure, au regard des éventuels risques juridiques ou autres, de la nécessité d'informer ou non les tiers concernés par cette sous-traitance et notamment les clients;
- La confidentialité des données doit être garantie en permanence, sauf consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps;
- L'établissement qui a l'intention de sous-traiter une activité matérielle doit obtenir l'autorisation préalable de la CSSF. Une notification à la CSSF, justifiant que les conditions fixées dans la présente circulaire sont respectées, est suffisante lorsque l'établissement recourt à un établissement de crédit

luxembourgeois ou à un PSF de support selon les articles 29-1, 29-2, 29-3 et 29-4 de la LSF;

- L'accès de la CSSF, du réviseur d'entreprises agréé et des fonctions de contrôle interne de l'établissement aux informations relatives aux activités sous-traitées doit être garanti en vue de leur permettre d'émettre une opinion fondée sur l'adéquation de la sous-traitance. Cet accès inclut que les précités peuvent également vérifier les données pertinentes détenues par un partenaire externe et, dans les cas prévues par la législation nationale, ont le pouvoir de mener des contrôles sur place chez un partenaire externe. L'opinion précitée peut, le cas échéant, se baser sur les rapports du réviseur externe du sous-traitant.

183. L'établissement qui sous-traite appuie sa décision de sous-traiter sur une analyse préalable et approfondie, démontrant qu'elle n'entraîne pas de délocalisation de l'administration centrale. Celle-ci portera au moins sur une description circonstanciée des services ou activités à sous-traiter, sur les effets attendus de la sous-traitance ainsi que sur une évaluation approfondie des risques du projet de sous-traitance envisagé sur le plan des risques financiers, opérationnels, légaux et de réputation.

184. Une attention particulière doit être portée à la sous-traitance d'activités critiques au niveau desquelles la survenance d'un problème pourrait avoir un effet significatif sur la capacité de l'établissement à respecter les exigences réglementaires, voire à poursuivre son activité.

185. Une attention particulière doit être accordée aux risques de concentration et de dépendance qui apparaissent lorsque de larges parties d'activités ou de fonctions importantes sont sous-traitées à un prestataire unique pendant une période prolongée.

186. Les établissements doivent prendre en compte les risques associés aux «chaînes» de sous-traitance (lorsqu'un prestataire sous-traite une partie des activités sous-traitées à d'autres prestataires). A cet égard ils accordent une attention particulière à la sauvegarde de l'intégrité du contrôle interne et externe. En outre, l'établissement veillera à fournir à la CSSF tous les éléments permettant de montrer que le processus de sous-traitance en cascade est maîtrisé.

187. La politique en matière de sous-traitance tient compte de l'impact de la sous-traitance sur les activités et les risques de l'établissement. Elle fixe les exigences de *reporting* auxquelles sont soumis les prestataires et le dispositif de contrôle que l'établissement met en place à leur égard pour la durée intégrale de la sous-traitance. La sous-traitance ne peut en aucun cas avoir pour effet de contourner des restrictions réglementaires ou des mesures prudentielles de la CSSF ou d'entraver la surveillance par la CSSF.

188. Une attention particulière doit être accordée aux aspects de continuité et au caractère révocable de la sous-traitance. L'établissement doit être en mesure de continuer à fonctionner normalement en cas d'événements exceptionnels ou de crise. A ce titre, les contrats de sous-traitance ne contiennent pas de clause de résiliation ou d'arrêt des prestations en raison de l'application à l'établissement de mesures d'assainissement ou d'une procédure de liquidation telles que prévues à la partie IV de la LSF. L'établissement prendra également les précautions qui

s'imposent afin d'être à même de transférer de manière adéquate les services sous-traités à un autre fournisseur ou de les reprendre en gestion propre, chaque fois que la continuité ou la qualité de la prestation de service risque d'être compromise.

189. Pour chaque activité sous-traitée, l'établissement désignera parmi ses employés une personne qui aura la responsabilité de la gestion de la relation de sous-traitance ainsi que la charge de gérer l'accès aux données confidentielles.

Section 7.4.2. Exigences particulières en matière de sous-traitance dans le domaine informatique

190. L'établissement met en place une politique informatique qui couvre l'ensemble des activités informatiques réparties entre l'établissement et son ou ses sous-traitants. L'organisation informatique est adaptée de manière à intégrer les activités sous-traitées au bon fonctionnement de l'établissement et le manuel de procédures est adapté en conséquence. Le plan de continuité de l'établissement est établi en cohérence avec le plan de continuité de son ou ses sous-traitants.

191. La politique de l'établissement en matière de sécurité des systèmes d'information prend en compte la sécurité individuelle mise en place par son ou ses sous-traitants, afin de s'assurer notamment de la cohérence de l'ensemble.

192. La sous-traitance en matière informatique peut porter sur des services de conseil, de développement et de maintenance (sous-section 7.4.2.2), des services d'hébergement (sous-section 7.4.2.3) ou des services de gestion/d'opération des systèmes informatiques (sous-section 7.4.2.1).

Sous-section 7.4.2.1. Services de gestion/d'opération des systèmes informatiques

193. Les établissements peuvent recourir contractuellement à des services de gestion/d'opération de leurs systèmes :

- Au Luxembourg, uniquement auprès:
  - d'un établissement de crédit ou d'un professionnel financier disposant d'un agrément de PSF de support selon les articles 29-3 et 29-4 de la LSF (statut d'opérateurs de systèmes informatiques primaires du secteur financier ou statut d'opérateurs de systèmes informatiques secondaires et de réseaux de communication du secteur financier);
  - d'une entité du groupe auquel l'établissement appartient et qui traite exclusivement des opérations de groupe, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible concernant les clients autres que des clients institutionnels, sauf s'il existe un consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps; concernant les clients institutionnels, les spécificités de cette sous-traitance doivent être explicites dans le contrat.
- A l'étranger, auprès:

- d’une entité du groupe auquel l’établissement appartient, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible concernant les clients autres que des clients institutionnels, sauf s’il existe un consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d’un avis éclairé concernant l’intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l’information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps ; concernant les clients institutionnels, les spécificités de cette sous-traitance doivent être explicites dans le contrat.

Sous-section 7.4.2.2. Services de conseil, de développement et de maintenance

194. Les services de conseil, de développement et de maintenance peuvent être contractés avec tout prestataire informatique, y compris un service informatique du groupe auquel l’établissement appartient ou un PSF de support.

195. L'interdiction d'accéder à des données confidentielles vaut pour des tiers sous-traitants autres que les PSF de support qui fournissent des services de conseil, de développement ou de maintenance. Ces tiers doivent intervenir par défaut hors du système informatique de production. Si une situation exceptionnelle rend nécessaire une intervention sur le système de production et que l'accès à des données confidentielles ne peut pas être évité, l’établissement doit veiller à ce que le tiers en question soit surveillé tout au long de sa mission par une personne de l’établissement en charge de l'informatique. Un accord exprès de l’établissement est nécessaire pour chacune des interventions sur le système de production, à l’exception des interventions réalisées par un PSF de support dans le cadre de son mandat.

196. Toute modification des fonctionnalités des applications par un tiers - autres que des modifications liées à de la maintenance corrective – doit être soumise pour accord à l’établissement, préalablement à sa mise en production.

197. L’établissement s'assurera qu'en cas de nécessité, il n'y ait aucun obstacle juridique pour avoir accès aux programmes d'exploitation qui ont été développés par un tiers sous-traitant. Ce but peut être atteint notamment lorsque l’établissement est juridiquement propriétaire des programmes. L’établissement s’assurera de la possibilité de poursuivre l’exploitation des applications critiques à l’activité en cas de défaillance du sous-traitant, pour une période compatible avec un transfert de cette sous-traitance vers un autre sous-traitant ou une reprise en mains propres des applications concernées.

Sous-section 7.4.2.3. Services d’hébergement et propriété de l’infrastructure

198. L’infrastructure informatique peut appartenir à l’établissement ou être mis à disposition par le sous-traitant.

Lorsque l’infrastructure informatique contient des données confidentielles, seul le personnel du PSF de support peut indifféremment travailler dans ses locaux ou ceux du professionnel financier sans encadrement particulier de la part du personnel de l’établissement, à condition que la prestation relève de l’article 41(5) de la LSF et fasse l’objet d’un contrat de service permettant cette autonomie. Lorsque le sous-traitant n’est pas PSF de support, il ne peut intervenir sur

l'infrastructure de l'établissement sans être accompagné tout au long de sa mission par une personne de l'établissement en charge de l'informatique.

Lorsque l'infrastructure informatique ne contient pas de données confidentielles, un accord exprès de l'établissement est nécessaire pour chacune des interventions sur l'infrastructure informatique par un tiers, à l'exception des interventions réalisées par un PSF de support dans le cadre de son mandat.

199. Il n'est pas exigé que le centre de traitement soit physiquement localisé auprès de l'entité contractuellement responsable de la gestion des systèmes informatiques. Que le centre de traitement soit au Luxembourg ou à l'étranger, il est donc possible que l'hébergement du site soit confié à un autre prestataire que celui qui preste les services de gestion des systèmes informatiques. Dans ce cas l'établissement doit s'assurer que les principes énoncés dans le présent sous-chapitre sont respectés par l'entité contractuellement responsable de la gestion des systèmes informatiques et que le processus de sous-traitance en cascade est maîtrisé.

200. Lorsque le centre de traitement est au Luxembourg, il peut être logé auprès d'un prestataire autre qu'un établissement de crédit ou un PSF de support, à condition que celui-ci n'ait aucun accès physique et logique sur les systèmes de l'établissement.

201. Lorsque le centre de traitement est à l'étranger, aucune donnée confidentielle de nature à identifier un client de l'établissement ne peut y être stockée, à moins d'être cryptée et à condition que le décryptage ne puisse se faire qu'au sein de l'établissement ou d'un PSF de support dans le cadre de sa prestation ou si l'ensemble des clients de l'établissement remplissent les conditions de consentement explicite et éclairé telles que définies au point 193.

Section 7.4.3. Exigences générales supplémentaires

202. Afin de permettre à l'établissement d'apprécier la fiabilité et l'exhaustivité des données produites par le système informatique ainsi que leur compatibilité avec les prescriptions comptables et de contrôle interne, il doit avoir parmi ses employés une personne ayant les connaissances nécessaires en matière informatique pour comprendre à la fois les effets que les programmes produisent sur le système comptable et les actions réalisées par le tiers dans le cadre des services rendus.

    L'établissement doit également disposer dans ses locaux d'une documentation suffisante des programmes utilisés

203. En cas de prestation de services informatiques par voie de télécommunication, l'établissement doit s'assurer :

    - que des mesures de protection suffisantes sont prises afin d'éviter que des personnes non autorisées ne puissent accéder à son système. L'établissement doit prévoir notamment que les télécommunications soient cryptées ou encore protégées selon d'autres moyens techniques disponibles de nature à assurer la sécurité des communications;
    - que la liaison informatique permet à l'établissement luxembourgeois d'avoir un accès rapide et non limité aux informations stockées dans l'unité de

traitement (par exemple grâce à un chemin d'accès et un débit adaptés et grâce à des solutions de redondance).

204. L'établissement doit s'assurer que les mécanismes de saisie, d'impression, de sauvegarde, de stockage et d'archivage garantissent la confidentialité des données.

205. La sous-traitance ne doit pas aboutir à transférer la fonction financière et comptable à un tiers. L'établissement disposera à la fin de chaque jour d'une balance de tous les comptes et de tous les mouvements comptables de la journée. Le système doit permettre de tenir une comptabilité régulière suivant les normes en vigueur au Luxembourg et donc de respecter les règles de forme et de fond imposées par la réglementation comptable luxembourgeoise.

206. Lorsque l'établissement opère à l'étranger en recourant aux services d'intermédiaires professionnels (même s'ils font partie du groupe auquel l'établissement appartient) ou lorsqu'il y dispose de succursales ou de bureaux de représentation, tout accès par ces intermédiaires ou les représentants et employés de ces bureaux et succursales à son système d'informations au Luxembourg doit faire l'objet d'une autorisation par la CSSF.

Section 7.4.4. Documentation

207. Toute sous-traitance d'activités matérielles ou non, y compris celle qui est réalisée au sein du groupe auquel l'établissement appartient, s'inscrit dans une politique écrite et nécessitant une approbation de la direction autorisée, incluant des plans d'urgence et des stratégies de sortie. Tout accord de sous-traitance fait l'objet d'un contrat officiel et détaillé (cahier des charges inclus).

208. La documentation écrite fournit également une description claire des responsabilités des deux parties ainsi que les moyens de communication clairs, assortis d'une obligation pour le prestataire de services externe de signaler tout problème important ayant un impact sur les activités sous-traitées, ainsi que toute situation d'urgence.

209. Les établissements prennent les dispositions nécessaires pour assurer que les fonctions de contrôle interne ont accès à tout moment et sans encombre à toute documentation relative aux activités sous-traitées et que ces fonctions gardent la pleine possibilité d'exercer leurs contrôles.

Chapitre 8. Reporting légal

210. Pour les établissements de crédit, le rapport ICAAP et l'attestation de conformité émis par la direction autorisée suivant le point 61 ainsi que les rapports de synthèse des fonctions de contrôle interne suivant le point 116 sont communiquées à la CSSF ensemble avec le projet des comptes annuels à publier (« procédure VISA »). Pour les entreprises d'investissement, ces informations sont soumis à la CSSF dans le mois qui suit la tenue de l'assemblée générale ordinaire ayant approuvé les comptes annuels. Les informations en question sont à établir en français, allemand ou anglais.

Partie III. Gestion des risques

Chapitre 1. Principes généraux en matière de mesure et de gestion des risques

Sous-chapitre 1.1. La gestion des risques

211. L'appréciation des risques se fait sur base d'une analyse objective et critique, propre à l'établissement. Elle ne peut pas reposer uniquement sur des évaluations externes.

212. L'établissement doit explicitement refléter l'ensemble de ses différents risques dans son dispositif de gouvernance interne comprenant en particulier les stratégies et politiques en matière de fonds propres et de réserves de liquidité. Il détermine en particulier ses niveaux de tolérance à l'égard de tous les risques qu'il encourt.

213. La politique de risque explique comment les différents risques sont détectés, mesurés, déclarés, gérés, limités et contrôlés. Elle fixe le processus d'approbation spécifique qui règle la prise de risques (et la mise en œuvre de mesures d'atténuation éventuelles) ainsi que les processus de mesure et de déclaration qui garantissent que l'établissement dispose en permanence d'une vue exhaustive sur l'ensemble de ses risques.

214. Les établissements se dotent d'un système de limites internes et de seuils d'alerte relatifs à l'ensemble de leurs risques.

215. Les risques envers des parties liées sont à traiter sur le plan interne comme des risques envers des parties tierces. Le dispositif de gouvernance interne leur est applicable dans tous ses éléments.

Sous-chapitre 1.2. La mesure des risques

216. Le dispositif de mesure et de déclaration des risques permet à l'établissement d'obtenir les vues agrégées nécessaires en vue de gérer et de contrôler l'ensemble des risques de l'établissement et des entités (structures) juridiques qui le composent.

217. Les décisions en matière de prise de risques et de stratégies et politiques de risques tiennent compte des limites théoriques et pratiques inhérentes aux modèles, méthodes et mesures quantitatives de risque ainsi que de l'environnement économique dans lequel ces risques s'inscrivent.

218. En règle générale, les techniques de mesure de risques mises en œuvre par un établissement reposent sur des choix, des hypothèses et des approximations. Il n'existe pas de mesure absolue.

    Par conséquent, les établissements doivent éviter l'excès de confiance placé dans une méthodologie ou un modèle spécifique. Les techniques de mesure de risques employées doivent toujours faire l'objet d'une validation interne, indépendante, objective et critique, et les mesures de risques qui sont issues de ces techniques sont à apprécier de manière critique et à utiliser avec discernement et prudence par tout le personnel, la direction autorisée et le conseil d'administration de l'établissement. Il y a lieu de compléter les évaluations de risque quantitatives par des approches qualitatives, y compris des jugements d'experts (indépendants).

Chapitre 2. Risques de concentration

219. Les risques de concentration résultent notamment de positions importantes (« concentrées ») sur des clients ou contreparties respectivement des groupes de clients ou contreparties liés, y compris des parties liées, sur des pays ou des secteurs (industries) ainsi que sur des produits ou des marchés spécifiques (concentration intra-risque). Ces positions peuvent être des postes d'actif, de passif ou de hors-bilan, mais les risques de concentration ne se réfèrent pas nécessairement à des postes inscrits au bilan ou hors-bilan. Par ailleurs, les risques de concentration peuvent être le résultat de différents risques (risque de crédit, risque de marché, risque de liquidité, risques opérationnels ou encore risques systémiques) qui se combinent (concentration inter-risques).

    Les concentrations intra-risques ou inter-risques peuvent se matérialiser par des pertes économiques et financières ainsi que par un impact significatif et négatif sur le profil de risque de l'établissement.

220. Les points 211 à 215 s'appliquent en particulier aux risques de concentration.

Chapitre 3. Risque de crédit

Sous-chapitre 3.1. Principes généraux

221. Chaque prise de risque de crédit doit faire l'objet d'une analyse écrite qui porte au moins sur la solvabilité du débiteur, sur le plan de remboursement et sur la capacité de remboursement de l'emprunteur sur toute la durée de l'emprunt. Les établissements prennent en compte le niveau d'endettement global de l'emprunteur.

    Les remboursements réguliers ne peuvent dépasser un montant qui ne laisserait à l'emprunteur un revenu disponible approprié. Une marge de sécurité raisonnable doit être prévue, en particulier pour absorber une hausse des taux d'intérêt.

222. Chaque prise de risque de crédit doit faire l'objet d'un processus décisionnel prédéfini qui englobe également une instance différente de la fonction commerciale.

223. Pour les prises de risque de crédit de faible importance, il est admissible que les établissements mettent en place un processus d'octroi qui leur permet de contrôler ces prises de risques dans leur ensemble sans nécessairement passer par les processus décisionnels et analyses individuelles tels que visés aux points 223 et 224.

    Il appartient aux établissements de définir en interne la notion de risque de crédit de « faible importance » pour les besoins du premier paragraphe. Cette définition s'oriente en particulier à la capacité de l'établissement à gérer, à supporter et à contrôler ces risques.

224. Les établissements disposent de politiques claires qui définissent les mesures à prendre lorsqu'un débiteur ne respecte pas ou signale à la banque qu'il n'est plus en mesure de respecter les clauses contractuelles de son engagement, notamment les différentes échéances de paiement.

225. Chaque décision de restructuration d'un crédit fait l'objet du processus décisionnel énoncé aux points 221 à 223. Les établissements maintiennent une liste reprenant l'ensemble des crédits restructurés.

Les restructurations visées sont celles qui sont liées à une détérioration de la solvabilité du débiteur. Elles comprennent notamment l'octroi de prorogations, de reports, de renouvellements ou de réaménagements de conditions de crédit, y compris le plan de remboursement.

226. Les établissements disposent d'un solide dispositif pour la détection et la gestion des engagements en retard de paiement. Les engagements en retard de paiement sont les engagements dont les échéances contractuelles définies pour le paiement du capital et/ou des intérêts sont dépassées.

Les établissements disposent d'un solide dispositif pour la détection, la gestion et le provisionnement des engagements « douteux ». Il s'agit de l'ensemble des engagements « en défaut » au sens de la partie VII, sous-section 3.4.2.2, des circulaires CSSF 06/273 et CSSF 07/290 qui définissent le défaut en termes de retard de paiement significatif (supérieur à 90 jours) ou d'indication de paiement improbable (« unlikeliness to pay »).

227. Les établissements doivent maintenir une liste des engagements douteux sur un débiteur ou groupe de débiteurs liés. Ces engagements font l'objet d'une revue périodique et objective qui doit permettre à l'établissement de reconnaître et d'effectuer les provisions et dépréciations d'actifs qui s'imposent.

Sous-chapitre 3.2. Crédits immobiliers résidentiels aux particuliers

Précision :
Pour les établissements actifs sur le marché domestique, il existe généralement une exposition concentrée sur le marché immobilier luxembourgeois. Un retournement significatif de ce marché, très difficile à prédire par ailleurs, serait de nature à porter atteinte à la stabilité financière de ces établissements et à impacter négativement l'image de la place financière luxembourgeoise dans son ensemble. Il importe dès lors que les établissements mettent en œuvre des politiques prudentes en matière d'octroi de crédits immobiliers, conformément au sous-chapitre 3.1 et au point 228. Par ailleurs, les établissements doivent disposer de fonds propres suffisants pour faire face à des développements adverses du marché immobilier résidentiel. Les exigences codifiées au point 229 entendent ainsi renforcer la stabilité financière de ces établissements par le biais d'exigences de fonds propres réglementaires dûment ajustées pour le risque. Ces exigences constituent un renforcement des règles actuelles contenues dans la circulaire CSSF 06/273 suivant les leçons tirées des épisodes récentes de crises financières. Ainsi, suivant le premier tiret du point 229, les établissements utilisant l'approche standard pour le risque de crédit ne peuvent appliquer dorénavant le taux de pondération préférentiel de 35% qu'aux seules parts de leurs crédits hypothécaires dont le rapport « loan-to-value » (LTV) est inférieur à 80% (crédits dont « la valeur du bien immobilier dépasse de 25% au moins celle de l'exposition »). Ainsi un crédit hypothécaire, qui remplit toutes les conditions d'éligibilité de la section 2.2.7.1 de la partie VII de la circulaire CSSF 06/273 (exposition sur la clientèle de détail pondérée à 75%) et les critères de la section 2.2.8.1 de la partie VII de cette même circulaire (pondération préférentielle à 35%) à l'exception du nouveau

critère 41, lit. d) qui limite le LTV à 80%, est dorénavant pondéré pour les besoins de la détermination des exigences de fonds propres réglementaires à (0,8/LTV)*35%+((LTV-0,8)/LTV)*75% au lieu de 35%. La part du crédit dépassant 80% de la valeur de l'objet immobilier est à pondérer suivant la classe d'exposition sous-jacente. Dans le cas sous rubrique, l'exposition satisfait tous les critères d'appartenance aux expositions sur la clientèle de détail et la pondération à risque s'établit par conséquent à 75%. Pour la détermination du LTV, les établissements peuvent prendre en considération tous les facteurs d'atténuation du risque - apport personnel direct de la part de l'emprunteur ou encore intervention de tiers par le biais d'apports, de sûretés réelles ou encore de garanties réelles ou personnelles dans les conditions prévues à la partie IX de la circulaire CSSF 06/273 (« reconnaissance des techniques d'atténuation du risque de crédit »).Pour les établissements utilisant l'approche fondée sur les notations internes et suivant le deuxième tiret du point 229, le seuil du « plancher » pour le taux de perte en cas de défaut est maintenu à 10% après le 31 décembre 2012.
Ces établissements doivent également soumettre leur adéquation réglementaire de fonds propres à un test d'endurance qui respecte au moins les paramètres inscrits au troisième tiret du point 229.

228. Les établissements appliquent une politique d'octroi de crédits prudente qui est de nature à préserver leur stabilité financière indépendamment de l'évolution du marché immobilier résidentiel. Cette politique s'articule notamment autour d'un rapport sain entre le montant du crédit accordé et la valeur des garanties obtenues (« loan-to-value »), y compris l'hypothèque sur l'immeuble sous-jacent.

229. La partie VII de la circulaire CSSF 06/273 est modifiée comme suit :

- Au point 41, lit. d), le texte «, d'une marge substantielle,» est remplacé par « de 25% au moins»;
- Au point 176, le début de phrase « Jusqu'au 31 décembre 2012, » est supprimé. Dans le titre du paragraphe 3.2.4.2.3., le mot « transitoire » est supprimé;
- Au point 257, la troisième phrase « Il doit être pertinent et raisonnablement prudent, incorporant au moins les conséquences de scénarios de récession économique légère » est remplacée par « Il doit être pertinent et refléter les conséquences d'un scénario de récession économique sévère mais plausible ». Enfin, est inséré au point 257 un deuxième paragraphe qui a la teneur suivante : « Pour les besoins du premier paragraphe, le test d'endurance portant sur les expositions sur la clientèle de détail garanties par un bien immobilier résidentiel présuppose un accroissement d'au moins 50% des probabilités de défaut et un taux de perte en cas de défaut d'au moins 20% ».

Sous-chapitre 3.3. Crédits aux promoteurs immobiliers

230. Chaque financement d'un projet de promotion immobilière doit prévoir au moment de l'octroi du crédit une date de commencement du remboursement du principal. Cette date ne peut pas dépasser un délai raisonnable par rapport au début du financement du projet. Un dépassement de ce délai implique automatiquement

le classement du dossier dans la liste des crédits restructurés (voir le point 225) et le provisionnement intégral des intérêts impayés.

Le financement de la promotion immobilière ne doit pas se faire sur simple notoriété du promoteur. Il doit être couvert, en sus de l'hypothèque sur l'objet financé, par une garantie personnelle du promoteur à moins que d'autres garanties ou sûretés ne couvrent significativement le coût total de l'objet financé.

Les établissements se fixent une limite interne pour l'exposition agrégée qu'ils encourent sur le secteur de la promotion immobilière. Sans préjudice des règles applicables en matière de grands risques (partie XVI de la circulaire CSSF 06/273), les garanties bancaires d'achèvement peuvent être exclues de cette limite agrégée pour autant que les frais d'achèvement sont adéquatement couverts par des taux de prévente ou de pré-location. Cette limite doit être en saine proportion avec leurs fonds propres réglementaires.

Chapitre 4. Tarification du risque (« Risk Transfer Pricing »)

231. L'établissement met un œuvre un mécanisme de tarification pour l'ensemble des risques encourus. Ce mécanisme, qui est intégré au dispositif de gouvernance interne, sert d'incitant à l'allocation efficace des ressources financières conformément à la tolérance à l'égard du risque et au principe d'une gestion saine et prudente des affaires.

232. Le mécanisme de tarification est approuvé par la direction autorisée et surveillé par la fonction de contrôle des risques. Les prix de transfert doivent être transparents et communiqués aux employés concernés. La comparabilité et la cohérence des systèmes des prix de cession interne utilisées au sein du groupe doit être assurée.

233. L'établissement élabore un système complet et efficace de prix de cession interne pour la liquidité. Ce système intègre tous les coûts, avantages et risques de la liquidité.

Chapitre 5. Gestion patrimoniale privée (« banque privée »)

234. Les établissements disposent de processus solides pour garantir que les relations d'affaires avec leurs clients sont conformes aux contrats conclus avec ces clients. Cet objectif peut être atteint au mieux lorsque les activités de gestion discrétionnaire, de gestion conseil et de simple exécution sont séparées d'un point de vue organisationnel.

235. Les établissements disposent de processus solides pour garantir le respect des profils de risque des clients, dans le but notamment de respecter les exigences découlant de la réglementation « MiFID ».

236. Les établissements disposent de processus solides pour garantir la communication d'informations correctes aux clients sur l'état de leurs avoirs. La production et la distribution des relevés de comptes et de toute autre information sur l'état des avoirs doivent être séparées de la fonction commerciale.

237. Les versements et retraits d'objets de valeur (par exemple les espèces et titres au porteur) doivent être effectués ou contrôlés par une fonction séparée de la fonction commerciale.

238. La modification des données signalétiques des clients doit être effectuée ou contrôlée par une fonction indépendante de la fonction commerciale.

239. Si un client achète un produit dérivé négocié sur un marché organisé, l'établissement répercute sans délais sur ce client (au moins) les appels de marge à fournir par l'établissement.

240. Les établissements doivent disposer d'un processus solide d'encadrement des crédits et dépassements en compte courant dans le cadre de l'activité de banque privée. Les garanties financières couvrant ces crédits doivent être suffisamment diversifiées et liquides. Dans le but de disposer d'une marge de sécurité adéquate, des décotes prudentes doivent être appliquées en fonction de la nature des garanties financières. Les établissements doivent disposer d'un « early warning system » indépendant de la fonction commerciale qui organise la surveillance de la valeur des garanties financières et déclenche le processus de liquidation des garanties financières. Il doit être assuré que le processus de liquidation soit déclenché suffisamment à temps et en tout cas avant que la valeur des garanties ne devienne inférieure au crédit. Les contrats avec les clients doivent décrire clairement la procédure déclenchée en cas d'insuffisance des garanties.

Chapitre 6. Risques liés aux entités shadow banking

241. Ce chapitre s'applique uniquement aux établissements auxquels s'applique la quatrième partie (grands risques) du règlement (UE) n° 575/2013, conformément au niveau d'application prévu à la première partie, titre II, dudit règlement.

Sous-chapitre 6.1. Mise en œuvre de principes de contrôle interne solides

~~241.~~242. Les établissements mettent en place un cadre interne dédié permettant de recenser, de gérer, de contrôler et d'atténuer les risques liés aux expositions sur les entités dites « entités du système bancaire parallèle » (« entités shadow banking »[13]) conformément aux EBA/GL/2015/20.

243. Les établissements appliquent un seuil de matérialité dédié pour identifier les expositions sur des entités shadow banking. Conformément aux EBA/GL/2015/20, toute exposition individuelle sur une entité shadow banking qui est supérieure ou égale à 0,25%[14] des fonds propres éligibles de l'établissement[15], après prise en compte des effets d'atténuation du risque de crédit et des exemptions[16], doit être prise en considération et ne peut pas être considérée comme une exposition de « faible importance ».

244. Les établissements veillent à ce que les risques éventuels pour l'établissement en raison de leurs différentes expositions sur des entités shadow banking soient pris en compte de manière adéquate dans le processus d'évaluation de l'adéquation du capital interne (ICAAP) de l'établissement et dans la planification du capital.

---

[13] Les entités shadow banking sont définies au paragraphe 11 « Définitions » des EBA/GL/2015/20. Il s'agit des entreprises exerçant une ou plusieurs activités d'intermédiation de crédit et qui ne sont pas considérées comme des « entreprises exclues » au sens dudit paragraphe. Par « activités d'intermédiation de crédit », il y a lieu d'entendre les entités effectuant des « activités non bancaires comprenant la transformation d'échéances, la transformation de liquidité, le financement d'investissement par effet de levier (leverage) et le transfert de risque de crédit ou des activités similaires ».

[14] Au sens de la définition des « Expositions sur des entités du système bancaire parallèle » du paragraphe 11 des EBA/GL/2015/20.

[15] Au sens de l'article 4, paragraphe 1, point 71, du règlement (UE) n° 575/2013.

[16] i) Effets d'atténuation du risque de crédit conformément aux articles 399 et 403 du règlement (UE) n° 575/2013,
ii) Exemptions prévues aux articles 400 et 493, paragraphe 3 du règlement (UE) n° 575/2013.

Sous-chapitre 6.2. Application de limites quantitatives

245. Les établissements limitent leurs expositions sur des entités shadow banking conformément à l'une des deux approches (approche de base ou approche de repli) telles que définies dans les orientations EBA/GL/2015/20.

246. Conformément à l'approche de base, les établissements doivent fixer une limite agrégée pour leurs expositions sur des entités shadow banking par rapport à leurs fonds propres éligibles.

247. Dans sa fixation d'une limite agrégée pour les expositions sur des entités shadow banking, chaque établissement doit tenir compte de :

- Son modèle d'entreprise, de son cadre de gestion du risque et de son profil d'appétence au risque ;
- La taille de ses expositions actuelles sur des entités shadow banking par rapport à ses expositions totales et par rapport à ses expositions totales sur des entités réglementées du secteur financier.
- L'interconnexion entre entités shadow banking, d'une part, et entre les entités shadow banking et l'établissement, d'autre part.

248. Indépendamment de la limite agrégée et en plus de celle-ci, les établissements doivent fixer des limites plus strictes pour leurs expositions individuelles sur des entités shadow banking.

249. Lorsqu'ils fixent ces limites, dans le cadre de leur processus d'évaluation interne, les établissements doivent tenir compte :

- Du statut réglementaire de l'entité shadow banking, et notamment de son statut ou non d'entité soumise à des exigences prudentielles ou de surveillance de quelque type que ce soit ;
- De la situation financière de l'entité shadow banking, comprenant, entre autres éléments, sa situation en matière de fonds propres, d'effet de levier et de liquidité ;
- Des informations disponibles concernant le portefeuille de l'entité shadow banking, notamment les prêts non productifs ;
- Le cas échéant, des preuves de l'existence d'éléments d'information disponibles concernant l'adéquation de l'analyse de crédit effectuée par l'entité shadow banking sur son portefeuille ;
- De l'éventuelle vulnérabilité de l'entité shadow banking face à la volatilité des prix des actifs ou de la qualité du crédit ;
- De la concentration d'activités d'intermédiation de crédit par rapport à d'autres activités de l'entité shadow banking ;
- De l'interconnexion entre entités shadow banking, d'une part, et entre les entités shadow banking et l'établissement, d'autre part ;
- De tout autre facteur pertinent recensé par l'établissement au titre d'expositions sur des entités shadow banking, la totalité des risques éventuels pour l'établissement en raison de ces expositions, et l'incidence éventuelle desdits risques.

250. Dans le cas où, les établissements ne sont pas en mesure d'appliquer l'approche de base telle que décrite ci-avant, les expositions agrégées sur des entités shadow banking doivent être soumises aux limites aux grands risques conformément à l'article 395 règlement (UE) n° 575/2013 (ci-après « approche de repli »).

251. L'approche de repli doit être appliquée comme suit :

- Si certains établissements ne peuvent satisfaire aux exigences concernant les processus et les mécanismes de contrôle efficaces ou la supervision par leur organe de direction, telles que prévues au chapitre 4 des EBA/GL/2015/20, ils doivent appliquer l'approche de repli à la totalité de leurs expositions sur des entités shadow banking (à savoir, la somme de leurs expositions sur des entités shadow banking).
- Si certains établissements peuvent satisfaire aux exigences concernant les processus et les mécanismes de contrôle efficaces ou la supervision par leur organe de direction, telles que prévues au sous-chapitre 6.1, mais ne peuvent réunir suffisamment d'informations pour leur permettre de fixer des limites appropriées, comme prévu à la section 6.2.1, ils ne doivent appliquer l'approche de repli qu'aux expositions sur des entités shadow banking pour lesquelles les établissements ne peuvent réunir suffisamment d'informations. L'approche de base telle que décrite à la section 6.2.1 doit être appliquée aux expositions restantes sur des entités shadow banking.

~~Chapitre 6.~~Chapitre 7. Risque de charge pesant sur les actifs (« asset encumbrance »)

~~242.~~252. Ce chapitre s'applique uniquement aux établissements de crédit.

~~243.~~253. Les établissements mettent en place des politiques de gestion des risques afin de définir leur approche de la charge pesant sur les actifs, de même que des procédures et contrôles qui garantissent que les risques associés à la gestion des garanties et à la charge pesant sur les actifs sont adéquatement identifiés, suivis et gérés. Il convient que ces politiques tiennent compte de leur modèle d'activité, des États membres dans lesquels ils opèrent, des spécificités des marchés du financement et de la situation macroéconomique. Ces politiques doivent être approuvées conformément aux dispositions du point 19.

~~244.~~254. Les établissements instituent un cadre de suivi général qui fournit des informations en temps utile, au moins une fois par an, à la direction autorisée et au conseil d'administration sur :

- le niveau, l'évolution et les types de charges pesant sur les actifs et sources connexes de charges pesant sur les actifs, telles que les financements garantis ou autres opérations;
- le montant, l'évolution et la qualité du crédit des actifs non grevés mais susceptibles de l'être, avec précision du volume des actifs disponibles pour être grevés;
- le montant, l'évolution et les types de charges pesant sur les actifs additionnelles, résultant des scénarios de crise (« charge pesant sur les actifs éventuelle » (« contingent encumbrance »)).

~~245.~~255. Les établissements incluent dans leurs plans de continuité des actions pour faire face à la charge pesant sur les actifs éventuelle résultant d'événements sources de tensions, à savoir de chocs plausibles bien que peu probables, y compris les dégradations des notations des établissements de crédit, les dévaluations des actifs nantis et les augmentations des exigences de marge.

Précision:

Le suivi du risque de charge sur les actifs sera réalisé au moyen de tableaux supplémentaires destinés à la déclaration des actifs grevés, qui viendront compléter le Règlement d'exécution (UE) n°680/2014, conformément aux exigences du règlement CRR concernant les exigences prudentielles applicables aux établissements de crédit. Un projet de tableaux provisoires a été publié par l'Autorité Bancaire Européenne le 24 juillet 2014 (EBA/ITS/2013/04/rev1).

~~Chapitre 7.~~Chapitre 8. Risque de taux d'intérêt inhérent aux activités autres que de négociation

256. ~~249~~. Dans leur mise en œuvre de l'article 14 (Risque de taux d'intérêt inhérent aux activités hors portefeuille de négociation) du Règlement CSSF N° 15-02 relatif au processus de contrôle et d'évaluation prudentiels s'appliquant aux établissements CRR, les établissements CRR[17] se conforment aux orientations que l'Autorité bancaire européenne a publiées en la matière~~.~~[18] Ne sont donc pas visées par le présent chapitre, les entreprises d'investissement qui ne sont pas des entreprises d'investissement CRR.

~~246.~~257. Ces orientations comprennent des exigences de haut niveau et des exigences détaillées qui visent les trois domaines suivants: les fonds propres internes alloués au risque de taux d'intérêt du portefeuille bancaire (« IRRBB 1 »), la mesure de ce risque (« IRRBB 2 » et « IRRBB 3 ») ainsi que le dispositif de gouvernance interne relatif au risque de taux d'intérêt du portefeuille bancaire (« IRRBB 4.1 » et « IRRBB 4.2 »).

Partie IV. Entrée en vigueur, mesures transitoires et dispositions abrogatoires

~~247.~~258. La présente circulaire est applicable à partir du 1er juillet 2013.

Par dérogation au premier paragraphe, les dispositions suivantes sont d'application à partir du 1er janvier 2014 :

- Section 4.1.2 (Composition et qualification du conseil d'administration);
- Section 4.1.4 en ce qui concerne les comités spécialisés, à l'exception du comité d'audit;

~~17 Le terme « établissement CRR » est défini à l'article 1er, paragraphe (1) du Règlement CSSF n° 15-02.~~

18 « ~~«~~ Orientations sur la gestion du risque de taux d'intérêt inhérent aux activités autres que de négociation ~~»~~ » (EBA/GL/2015/08) accessibles sur le site internet de l'EBA à l'adresse suivante : https://www.eba.europa.eu/-/eba-updates-guidelines-on-interest-rate-risk-arising-from-non-trading-activities

- Point 32 (Interdiction de cumuler les mandats de président du conseil d'administration et de directeur agréé);
- La nécessité de fixer par écrit les lignes directrices prévues aux tirets 4 à 8 du point 17.

~~248.~~259. Les circulaires IML 93/94 et CSSF 10/466 sont abrogées à partir du 1er juillet 2013.

~~249.~~260. Les circulaires IML 95/120, IML 96/126, IML 98/143, CSSF 04/155 et CSSF 05/178 ne sont plus applicables aux établissements de crédit et entreprises d'investissement à partir du 1er juillet 2013.

~~250.~~261. Mises à jour successives :

- Circulaire CSSF 13/563 ~~-~~ transposant les orientations de l'EBA en matière d'éligibilité des administrateurs, directeurs autorisés et responsables de fonctions clé du 22 novembre 2012 (Guidelines on the assessment of the suitability of members of the management body and key function holders - EBA/GL/2012/06) ainsi que les orientations du 6 juillet 2012 de l'ESMA concernant certains aspects de la directive MIF relatifs aux exigences à l'encontre de la fonction compliance (Guidelines on certain aspects of the MiFID compliance function requirements - ESMA/2012/388).

  Les orientations précitées sont disponibles sur le site de l'EBA (www.eba.europa.eu) et de l'ESMA (www.esma.europa.eu).

- Circulaire CSSF 14/597 transposant la recommandation du Comité Européen du Risque Systémique (CERS) sur le financement des établissements de crédit (CERS/2012/2) - sous-recommandation B concernant la mise en place d'un cadre général de gestion du risque de charge pesant sur les actifs (« asset encumbrance »).

  La recommandation précitée est disponible sur le site du CERS (www.esrb.europa.eu).

- Circulaire CSSF 16/642 transposant les orientations de l'EBA en matière de gestion du risque de taux d'intérêt inhérent aux activités autres que de négociation (*Guidelines on the management of interest rate risk arising from non-trading activities* - EBA /GL/2015/08).

- Circulaire CSSF 16/647 transposant les orientations de l'EBA en matière de limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013 (*Guidelines on limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) n° 575/2013* – EBA/GL/2015/20).

  Les orientations précitées sont disponibles sur le site de l'EBA (www.eba.europa.eu).

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON
Directeur

Simone DELCOURT
Directeur

Jean Guill
Directeur général

EBA/GL/2015/20

14 December 2015

Guidelines

Limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013

Contents

1. Executive Summary

Under Article 395(2) of Regulation (EU) No 575/2013, the EBA has a mandate to develop guidelines to set appropriate aggregate limits or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.

The global financial crisis has revealed previously unrecognised fault lines which can transmit risk from the shadow banking system to the regulated banking system, putting the stability of the entire financial system at risk.

From a microprudential perspective, shadow banking entities are generally not subject to the same standards of prudential regulation as core regulated entities such as institutions, do not provide protection to investors' investment from these entities' failures, and do not have access to central banks' liquidity facilities. To the extent that shadow banking entities carry out bank-like activities, exposures to such entities may therefore be inherently risky - and thus specific limits for individual and aggregate exposures could be warranted.

Macro prudentially, institutions' exposures to shadow banking entities could be of concern for different reasons. Here, institutions' exposures to such entities undertaking bank-like activity may lead to regulatory arbitrage concerns, and worries that core banking activity may migrate systematically away from the regulated sector 'into the shadows'. In order to seek profits, institutions may still actively seek ways to arbitrage the rules by funding shadow banking entities. These entities, which are potentially more vulnerable to runs and/or liquidity problems, tend to be highly correlated and interconnected with the banking sector, which leads to financial stability concerns.

To minimise the risks posed to institutions arising from their exposures to shadow banking entities, the guidelines lay down requirements for institutions to set limits, as part of their internal processes, on their individual exposures to shadow banking entities (alleviating primarily the microprudential concerns expressed above) and on their aggregate exposure to shadow banking entities (alleviating macroprudential concerns).

In the absence of a definition in Regulation (EU) No 575/2013 of the terms 'shadow banking entities', 'banking activities' and 'regulated framework', it has been necessary to develop a definition of those terms for the purposes of the guidelines. The definitions proposed are in line with the previous EBA Opinion and Report on the perimeter of credit institutions[1] and aim at capturing entities that are not subject to appropriate prudential regulation and supervision, and therefore pose the greatest risks.

1 The Opinion and Report are available here: http://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-perimeter-of-credit-institutions.

To better understand the relevance of institutions' exposures to shadow banking entities and the impact of potential limits, a data collection was conducted and the results published in a separate report. The scope of the data collection was, however, broader than the current scope of the guidelines so as to provide a sound basis for the calibration of any limits and to assist the European Commission's work in relation to its report on the appropriateness and impact of imposing limits on exposures to shadow banking entities under the last subparagraph of Article 395(2) of Regulation (EU) No 575/2013.

In prescribing the approach institutions should adopt for the purposes of setting appropriate individual and aggregate limits for exposures to shadow banking entities, these guidelines will establish a harmonised approach for mitigating the risks identified above and will also inform the European Commission's report.

Next steps

The guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report on whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from 01/01/2017.

2. Background and rationale

2.1 General background

1. Shadow banking can complement traditional banking by expanding valuable access to credit in support of economic activity or by supporting market liquidity, maturity transformation and risk sharing, thereby supporting growth in the real economy. For example, various types of non-bank funds have stepped in (often as intermediaries for insurance companies and pension funds) to provide long-term credit to the private sector while banks have been repairing their balance sheets and retrenching from certain activities[2]. Moreover, in the euro area, recent data shows that lending by shadow banks as a proportion of total lending is rising[3]. Research also suggests that shadow banking often enhances the efficiency of the financial sector by enabling better risk sharing and maturity transformation and by deepening market liquidity[4].

2. However, the global financial crisis has revealed previously unrecognised fault lines in the shadow banking system which put the stability of the financial system at risk. These include a heavy reliance on short-term wholesale funding and a general lack of transparency, which masked the increasing amounts of leverage, maturity and liquidity transformation in the run-up to the crisis, and in turn increased the vulnerability of shadow banking entities to runs. The subsequent fire sale of assets by such entities helped spread the stress to the traditional banking system.

3. A number of international regulatory initiatives relating to shadow banking have been undertaken and some are currently in progress. For example, in April 2011 the Financial Stability Board (FSB) published Recommendations to Strengthen Oversight and Regulation of Shadow Banking[5] and in April 2014 the Basel Committee on Banking Supervision (BCBS) published a revised supervisory framework for measuring and controlling large exposures, which includes exposures to shadow banking entities[6]. At the EU level, the Commission has adopted a proposal for a regulation aimed at increasing transparency of certain transactions outside the regulated banking sector[7]. Additionally, work has been undertaken to analyse the scope of the perimeter of credit

[2] See IMF Global Financial Stability Report, April 2014, available here: http://www.imf.org/external/pubs/FT/GFSR/2014/01/index.htm.

[3] See IMF Global Financial Stability Report, October 2014, available here: http://www.imf.org/external/pubs/ft/gfsr/2014/02/ ; and the Financial Stability Board's Global Shadow Banking Monitoring Report 2014, available here: http://www.financialstabilityboard.org/2014/11/global-shadow-banking-monitoring-report-2014/ .

[4] Claessens, Stijn, Zoltan Pozsar, Lev Ratnovski and Manmohan Singh, December 2012, 'Shadow Banking: Economics and Policy', IMF Staff Discussion Note SDN/12/12, International Monetary Fund, Washington, DC.

[5] The FSB's recommendations are available here: http://www.financialstabilityboard.org/2011/10/financial-stability-board-publishes-recommendations-to-strengthen-oversight-and-regulation-of-shadow-banking/.

[6] 'Supervisory framework for measuring and controlling large exposures - final standard', Basel Committee on Banking Supervision, Bank for International Settlements, April 2014.

[7] Proposal for a regulation of the European Parliament and of the Council on reporting and transparency of securities financing transactions, European Commission, January 2014.

institutions in the EU, the results of which are set out in the EBA's Opinion and Report on the perimeter of credit institutions[8]. At the international level, work led by the BCBS is under way on accounting and regulatory approaches to consolidation. The FSB is also conducting intensive monitoring of the shadow banking sector[9] and investigating financial stability risks from asset management activities[10].

2.1.1 Concerns regarding shadow banking entities

4. Whilst some activities carried out by shadow banking entities can have beneficial effects as regards the financing of the real economy and fostering growth, they also generate a number of specific risks from a prudential viewpoint that may warrant regulatory attention.

- *Run risk and/or liquidity problems*: Shadow banking entities are potentially vulnerable to runs (withdrawal of deposit-like assets due to panic, early redemptions due to a confidence crisis) and/or liquidity problems (liquidation of assets at fire sale prices), stemming from credit exposures, high leverage, and liquidity and maturity mismatches between assets and liabilities. These risks are usually exacerbated because shadow banking entities do not have sectoral liquidity backstops and are generally subject to less robust and comprehensive prudential standards and supervision.

- *Interconnectivity and spillovers:* Shadow banking entities tend to be highly correlated and interconnected with the regulated banking sector due to ownership linkages and explicit and implicit credit commitments and as direct counterparties. In times of stress this can, directly or indirectly, generate systemic risks through contagion effects both between shadow banking entities and between such entities and the regulated banking sector, leading to a flight to quality and fire sales of assets.

- *Excessive leverage and procyclicality*: The maturity mismatch and liquidity risks are exacerbated by shadow banking entities' ability to engage in highly leveraged or otherwise risky financial activities. Highly leveraged structures are more likely to become insolvent in the case of unexpected negative events due to inadequate loss-absorbing capacity, abrupt deleveraging and inability to roll over financing needs. The crystallisation of such events can trigger a confidence crisis in the regulated banking sector, leading to severe impairment of funding sources.

- *Opaqueness and complexity*: The opaque and complex nature of governance and ownership structures of shadow banking entities and their relationships with the regulated banking sector constitute vulnerabilities, since, during periods of stress, investors tend to retrench and flee to safe, high-quality and liquid assets. The inherent agency problem, caused by the separation of financial intermediation activities across multiple shadow banking entities, also

[8] The EBA's Opinion and Report are available here: https://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-perimeter-of-credit-institutions.

[9] See for example the FSB's Global Shadow Banking Monitoring Report 2014 as referred to in footnote 2.

[10] http://www.financialstabilityboard.org/2015/07/next-steps-on-the-nbni-g-sifi-assessment-methodologies/

contributes to vulnerabilities in the financial system. Furthermore, there is a lack of disclosure (regarding collateral, assets or value thereof), as such entities are generally unregulated or subject to less robust prudential regulation.

2.1.2 Legal mandate and definitions used

5. The EBA has the mandate under Regulation (EU) No 575/2013[11] to issue guidelines to set limits on institutions' exposures to shadow banking entities.

6. Article 395(2) of Regulation (EU) No 575/2013 reads as follows:

'*EBA shall, in accordance with Article 16 of Regulation (EU) No 1093/2010, taking into account the effect of the credit risk mitigation in accordance with Articles 399 to 403 as well as the outcomes of developments in the area of shadow banking and large exposures at the Union and international levels, issue guidelines by 31 December 2014 to set appropriate aggregate limits to such exposures or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.*

'In developing those guidelines, EBA shall consider whether the introduction of additional limits would have a material detrimental impact on the risk profile of institutions established in the Union, on the provision of credit to the real economy or on the stability and orderly functioning of financial markets.'

7. In the absence of a definition in Regulation (EU) No 575/2013 of the terms 'shadow banking entities', 'banking activities' and 'regulated framework', for the purposes of these guidelines, the EBA defines shadow banking entities as entities that:

   a. carry out credit intermediation activities, defined as bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities; and

   b. are neither within the scope of prudential consolidation nor subject to solo prudential requirements under specified EU legislation (or equivalent third country legal frameworks). Entities referred to in Article 2(5) and Article 9(2) of Directive 2013/36/EU[12], as well as other entities as defined in the guidelines ('excluded undertakings'), are also not to be regarded as shadow banking entities.

8. This approach is consistent with the EBA's Opinion and Report on the perimeter of credit institutions[13]. In particular, the guidelines do not prescribe an exhaustive list of activities that fall within the scope of credit intermediation activities. Instead, the description of 'credit

[11] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 321, 30.11.2013, p. 6).

[12] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[13] See footnote 8.

intermediation' adopted in the aforementioned Opinion and Report, which follows the approach prescribed by the FSB, has been adopted, as this best describes the types of activities undertaken by shadow banking entities. The FSB has identified the four key features of credit intermediation as: (a) maturity transformation (borrowing short and lending/investing on longer timescales); (b) liquidity transformation (using cash-like liabilities to buy less liquid assets); (c) leverage; and (d) credit risk transfer (transferring the risk of credit default to another person for a fee). Examples of entities carrying out credit intermediation include money market funds (MMFs), special-purpose vehicles (SPVs) engaged in securitisation transactions, securities and derivatives dealers, and companies engaged in factoring, leasing or hire purchase.

9. In order to assist institutions in identifying entities that are carrying out credit intermediation activities, the guidelines make it clear that entities carrying out one or more of the activities listed in the following points of Annex 1 of Directive 2013/36/EU shall be automatically regarded as carrying out credit intermediation activities: points 1 (taking deposits and other repayable funds), 2 (lending), 3 (financial leasing), 6 (guarantees and commitments), 7 (trading for own account or for account of customers in specified forms of financial instrument), 8 (participation in securities issues and the provision of services relating to such issues) and 10 (money broking). However, this should not be taken as an exhaustive list of activities within the scope of 'credit intermediation'. Rather, this approach simply confirms specific cases in which entities are to be positively identified as carrying out credit intermediation activities for the purposes of the guidelines.

10. The second limb of the definition of shadow banking entities for the purposes of the guidelines carves out certain entities from the scope of the definition (and therefore from the scope of the guidelines). These are entities that are subject to an appropriate and sufficiently robust prudential framework. For example, under this approach, credit institutions, investment firms, insurers and entities established in third countries which are subject to prudential requirements which are considered to be equivalent to those applied in the Union are out of the scope of the guidelines. Furthermore, entities subject to consolidated prudential supervision (whether as a result of EU legislation, applicable national legislation or an equivalent third country legal framework) are out of the scope of the guidelines.

11. Given this, the guidelines focus on institutions' exposures to entities that pose the greatest risks in terms of both the direct exposures institutions face and also the risk of credit intermediation being carried out outside the regulated framework (see further below). These entities include unregulated financial sector entities such as special-purpose entities (SPEs) and SPVs not covered by consolidated prudential supervision.

12. As regards funds, these tend to engage in maturity and liquidity transformation and are generally regarded as outside the traditional banking sector[14]. Therefore, *prima facie*, they should be within the scope of the definition of shadow banking entity.

[14] For example, see the FSB's Global Shadow Banking Monitoring Report 2014.

13. However, some funds are regulated pursuant to prudential frameworks similar to those applied to credit institutions and investment firms. In particular, in the EU the UCITS (Undertakings for Collective Investments in Transferable Securities) Directive (Directive 2009/65/EC) prescribes a robust set of requirements under which undertakings for collective investment in transferable securities, and their managers, operate. These include requirements on the asset manager (initial capital, own funds and internal control requirements) and the managed funds (e.g. limits to leverage and concentration). Therefore, such funds do not pose the same level of risk to institutions in terms of credit and step-in/bail-out risk (e.g. due to reputational, franchise and other risks) as unregulated funds.

14. Notwithstanding these requirements, it is proposed that all MMFs, regardless of whether they operate under the rules of Directive 2009/65/EC or others, should be within the scope of the definition of shadow banking entity for the purposes of these guidelines. This is because, as acknowledged by the European Commission in its proposal for a regulation on MMFs[15] (under negotiation), the average size of an MMF far exceeds the average size of a UCITS fund and, as acknowledged by the FSB and other institutions such as the International Organisation of Securities Commissions and the European Systemic Risk Board[16], the systemic risks posed by such funds (in particular having regard to their interconnectedness with the banking sector) have not been addressed to an adequate degree through existing regulatory measures. Therefore, at this stage (in particular, pending agreement on the Commission's legislative proposal) the EBA includes all MMFs within the scope of the definition of shadow banking entity.

15. Regarding the treatment of alternative investment funds (AIFs), the EBA has considered the feedback received during the consultation period as well as input from the European Securities Market Authority (ESMA) and the European Commission. The EBA acknowledges that AIFs are regulated indirectly, as a result of requirements imposed on their asset managers under Directive 2011/61/EU (the AIFMD), e.g. initial capital, own funds and internal controls requirements. However, the risks arising directly from the funds themselves are not mitigated in a satisfactory way from a prudential point of view. For example, leverage is strictly limited for UCITS funds: they can borrow only up to 10% of their assets provided that such borrowing takes place on a temporary basis[17]. However, similar leverage limitation does not apply to AIFs, although they

[15] The Commission's proposal is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.

[16] IOSCO's recommendations are available here: http://www.iosco.org/news/pdf/IOSCONEWS255.pdf.

The ESRB's recommendations are available here: https://www.esrb.europa.eu/pub/pdf/recommendations/2012/ESRB_2012_1.en.pdf?c9daf560cb3d72433ca237604eda38af.

[17] In most cases leverage is measured as a ratio between the fund exposure and its Net asset Value (NaV). Most UCITS are required to use the commitment approach, under which derivatives exposures are converted into equivalent cash positions. When UCITS engage in complex investment strategies or when the commitment approach does not adequately capture the market risk of their portfolio, they should use either the absolute or the relative Value at Risk (VaR). All AIFs are required to measure their exposure through the commitment method, similarly to UCITS. Under the commitment approach, UCITS exposure relating to derivative instruments cannot exceed the total net value of the portfolio. Eventually a UCITS using both external borrowing and derivatives can thus leverage up to 1.1 times its NaV (i.e. overall leverage of 2.1). For more sophisticated UCITS, the relative VaR approach does not measure the leverage of the strategies; rather it allows UCITS to double the risk of loss compared with a similar but unleveraged portfolio. Finally the VaR of a UCITS using the

must put in place risk management policies and are subject to stress testing and reporting obligations[18]. Given this, the EBA is of the view that only AIFs with limited leverage could be considered to fall outside the definition of 'shadow banking entities'. Article 111(1) of Delegated Regulation 231/2013 considers leverage to be employed on a substantial basis when the AIF exposure exceeds 300% of its net asset value. Furthermore, only AIFs which are not entitled to grant loans or purchase third parties' lending exposures onto their balance sheet should be excluded from the definition of 'shadow banking entities' for the purposes of these guidelines. On the contrary, AIFs which are entitled to grant loans carry out a typical banking activity outside the regulated banking system (i.e. Regulation (EU) No 575/2013 and Directive 2013/36/EU or comparable prudential regulation). These funds should therefore fall within the scope of the guidelines, as they act as substitutes for bank lending and could generate credit intermediation risks (i.e. runs and/or liquidity risk) without having a banking (or comparable) licence and they are not subject to harmonised rules on concentration risks, credit assessment, provisioning, etc.

16. Given this, all funds would be considered to fall within the scope of the definition of shadow banking entities except if they are non-MMF UCITS, AIFs meeting the criteria mentioned in the paragraph above or third country funds subject to requirements equivalent to the UCITS Directive.

17. Regarding the particular case of European Venture Capital Funds (EuVECAs), European Social Entrepreneurship Funds (EuSEFs) and European Long-Term Investment Funds (ELTIFs), the EBA is of the view that these funds should fall outside the definition of 'shadow banking entity' due to their type of activity, and should therefore be excluded from the scope of the guidelines.

18. This approach is consistent with the approach described in the EBA's Opinion and Report on the perimeter of credit institutions[19] and the general focus of the policy debate on shadow banking within the European Union and in international contexts[20].

2.1.3 Relation to other parts of the European rulebook

19. The guidelines should be applied independently from and in addition to the general large exposures framework as defined in Part Four of Regulation (EU) No 575/2013.

20. On 27 November 2014, Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council as regards regulatory technical standards for determining the overall exposure to a client or a group

---

absolute VaR approach cannot be greater than 20% of its NaV. The VaR approaches potentially allow higher leverage than the commitment approach, depending on the volatility of the underlying assets.

[18] For an overview of leverage measures and restrictions, see ECB (2015), 'Financial Stability Review, Box 7: Synthetic leverage in the investment fund sector', May 2015, pp. 92-94.

[19] See footnote 8.

[20] For example, see the Commission's (2013) Communication on shadow banking: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0614&from=EN; the IMF's 2014 Global Financial Stability Report: http://www.imf.org/external/pubs/ft/gfsr/2014/02/, which includes in Chapter 2 an assessment of the size and riskiness of shadow banking around the globe; and the Financial Stability Board's 2014 Global Shadow Banking Monitoring Report, available here: http://www.financialstabilityboard.org/2014/11/global-shadow-banking-monitoring-report-2014/.

of connected clients in respect of transactions with underlying assets entered into force. This regulation applies to all exposures through transactions with underlying assets, thus also including exposures that are within the scope of the guidelines.

21. In addition, the EBA is updating the guidelines on the identification of groups of connected clients under Article 4(1)(39) of Regulation (EU) No 575/2013, including providing greater clarity on how institutions and shadow banking entities can be economically interdependent.

22. The guidelines should be read in conjunction with supervisory powers under the Supervisory Review and Evaluation Process (SREP) of Pillar 2. The articulation between these guidelines and Pillar 2 is further developed in the following section.

23. Finally, the guidelines are developed having regard to the Commission's mandate under Article 395 of Regulation (EU) No 575/2013 to 'assess the appropriateness and the impact of imposing limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework' by 31 December 2015.

24. In developing the guidelines, the EBA is also mindful of other European and international workstreams in the area of shadow banking and large exposures. These include:

- An assessment by the European Commission of the current scope of application of the EU banking prudential rules, as part of the Commission's broader workstream on shadow banking[21]. The EBA provided an opinion on this matter, at the request of the Commission, in November 2014[22].

- Work by the BCBS, on the scope of consolidation for prudential regulatory purposes to ensure all banks' activities are appropriately captured in prudential regimes. A public consultation on the proposals is expected by the end of 2015.

- A peer review, to be launched by the FSB in 2015, regarding its member jurisdictions' implementation of the FSB's policy framework for shadow banks, as well as the results of the FSB's fifth shadow banking monitoring exercise in late 2015[23].

2.1.4 Rationale for limiting institutions' exposures to shadow banking entities

25. Potential risks could arise from institutions' exposures to shadow banking entities from both a microprudential and a macroprudential perspective.

26. A general concern is that institutions' exposures to shadow banking entities undertaking bank-like activity may also lead to regulatory arbitrage concerns, and worries that core banking activity may migrate systematically away from the regulated sector 'into the shadows'. A range of regulations are now in place to address some of the arbitrage risks relating to shadow banking entities that

[21] Shadow Banking – Addressing New Sources of Risk in the Financial Sector, European Commission, 4 November 2013.

[22] Opinion of the European Banking Authority on Matters Relating to the Perimeter of Credit Institutions, EBA/Op/2014/12, 27 November 2014.

[23] Updated G20 Roadmap towards Strengthened Oversight and Regulation of Shadow Banking in 2015, G20.

were observed during the financial crisis. For example, the risk weights on various forms of shadow banking exposures have increased. Nonetheless, as the regulatory regime for institutions tightens, the pressure for bank-like activity to be carried out elsewhere in the financial system increases.

27. From a microprudential perspective, banking activities such as maturity and liquidity transformation are inherently risky. For this reason, institutions are subject to robust prudential regulation, must participate in Deposit Guarantee Schemes and generally have access to central bank liquidity facilities. Shadow banking entities are generally unregulated or not subject to the same standards of prudential regulation as core regulated entities such as institutions, do not provide protection to investors' investment from these entities' failures and do not have access to central banks' liquidity facilities. To the extent that shadow banking entities carry out banking activities, exposures to such entities may therefore be inherently risky - and thus specific limits for individual and aggregate exposures are warranted.

28. Macro prudentially, institutions' exposures to shadow banking entities could be of concern for different reasons. Here the focus is on the role that institutions' funding of bank-like activity amongst shadow banking entities may play in increasing systemic risk across the financial system. One concern is that institutions' funding of large amounts of bank-like activity amongst shadow banking entities may result in an amplification of the credit cycle. Such a concern may arise from the observation that the flow of funds into such entities tends to be volatile. Moreover, the sharp accelerations of credit flows (and implicit exposures) into these entities can result in volatile (and potentially unsustainable) credit flows into the real economy. A limit on institutions' aggregate exposures to shadow banking entities could play a role in reducing the volatility of such flows.

29. Notwithstanding these microprudential and macroprudential risks, the EBA recognises that banking activities by some shadow banking entities can play a valuable role in providing alternative sources of funding to the real economy. Excessively reducing the availability of institutions' funding to these entities could therefore interfere with the flow of funds into the real economy. Moreover, the regulatory bodies, in the EU and at the global level, are still in the process of assessing the balance of risks and benefits that institutions' funding to different types of shadow banking entities represents. It is therefore considered premature to use the guidelines to introduce a quantitative limit to institutions' exposures to these entities at the individual or aggregate exposure level. Instead, the proposed intervention is designed to place the responsibility on the banking sector to demonstrate that the risks highlighted above are being managed effectively, in particular by improving, where necessary, the due diligence carried out before taking lending decisions, for instance to identify if the counterparty is carrying out credit intermediation and its regulatory status (see also sub-section 2.1.1, *Concerns regarding shadow banking entities*).

30. Under the guidelines, institutions should implement effective processes, as well as set internal aggregate and individual limits to exposures to individual shadow banking entities with an exposure value, after credit risk mitigation and exemptions, equal to or in excess of 0.25% of the institution's eligible capital as defined in Article 4(1)(71) of Regulation (EU) No 575/2013. The

materiality threshold of 0.25% of the institution's eligible capital reduces the burden of application of the guidelines, as it allows institutions to disregard immaterial exposures which are not likely to pose risks that would deserve special attention. The data collection accompanying these guidelines has shown that the number of exposures below this materiality threshold is very significant for most institutions: these exposures represent around 97% of the total number of exposures for the overall sample of institutions in the data collection.

31. The internal limits should be set using criteria which are laid down in the guidelines. The rationale for this approach ('the principal approach') is to make sure institutions have sufficient information about their counterparties in the shadow banking sector to make an informed assessment of their risk exposures to shadow banking entities as a whole, as well as of any individual exposure to shadow banking entities. It shall be noted that there is no necessary sequence for the setting of limits: i.e. institutions have to set both aggregate and individual limits, in any order.

32. Institutions that cannot use the principal approach for setting the internal limits as a result of their inability to take into account all the criteria, due to either an insufficient level of information about their exposures to shadow banking entities or the lack of effective processes to use that information, shall use an alternative approach ('the fallback approach') involving a set aggregate limit to all or some of their exposures to shadow banking entities. Where institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board as set out in Section 4 of the guidelines, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Section 5 of the guidelines, the fallback approach should only be applied to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach should be applied to the remaining exposures to shadow banking entities.

33. Although the results of the data collection provided relevant input to the calibration of the aggregate limit under the fallback approach, the EBA notes some important differences between the data collection and the guidelines: the scope of the data collection was broader than the current scope of the guidelines[24]; the data collection was conducted at the highest level of consolidation in a Member State or individual level if the consolidated level did not apply; and

[24] The data collection used the same definition of 'shadow banking entities' as included in the guidelines, with the following exceptions, where more granular data was collected:

a. The list of 'excluded undertakings' considered for the definition of 'shadow banking entity' in the guidelines extends beyond the one considered for the data collection (i.e. points (k), (m), (n), (o), and (p) of the list in the guidelines have not been considered 'excluded undertakings' for the purposes of the data collection). For example, institutions have been asked to report exposures to all investment funds, regardless of whether they are subject to the UCITS Directive or the AIFMD. Note that UCITS funds (other than money market funds) and alternative investment funds that meet certain requirements have been excluded from the scope of the guidelines.

b. Institutions have been asked to report exposures to all third party undertakings. Note that undertakings which are not supervised on a solo level, but supervised on a consolidated level in the Union or in a third country which has a regime at least equivalent to the one applied in the Union, have been excluded from the scope of the guidelines.

data simulations were done under the conservative assumption that the institution would apply the fallback approach to all of its exposures.

34. The main purpose of the fallback approach is to create certainty about the possibility of setting a limit for any institution; in particular, some institutions may not be able to apply all of the relevant criteria to use the principal approach. In that sense, the limit in the fallback approach can be seen as a way to ensure that these institutions apply a sufficiently tight limit to their exposures to shadow banking entities, for which institutions are not able to collect sufficient information that would enable them to understand and manage the risks of these exposures. The fallback approach can also work as an incentive for these institutions to improve their processes and control mechanisms concerning their exposures to shadow banking entities in order to be able to apply the criteria under the 'principal approach' to all their exposures to shadow banking entities.

35. All in all, the approach proposed in these guidelines requires institutions to set risk tolerance levels for exposures to shadow banking entities within their overall business model and risk management framework, under the supervision of the competent authority. In this regard, it is recognised that some institutions may have a higher risk appetite for these types of exposures and this can be accommodated within the guidelines once risks arising from these exposures are identified and appropriately mitigated. Given this, these guidelines are a first step to address the potential risks stemming from exposures to shadow banking entities. As already mentioned, the EBA has collected data about exposures to shadow banking entities in order to inform further work to be done on the topic by the Commission in accordance with its mandate under the last subparagraph of Article 395(2) of Regulation (EU) No 575/2013. The results of this data collection are presented in a separate report. As part of this mandate, the Commission may choose to propose imposing mandatory limits to exposures to shadow banking entities that are tighter than the limits currently laid down for large exposures in general. In any case, the EBA expects these guidelines to be a useful input to the Commission's report.

36. Under this approach, competent authorities will retain the ability to take supervisory measures to address any risks arising from exposures to shadow banking entities, as appropriate, and in particular to assess and challenge the internal limits and risk mitigation plans set by institutions.

37. The competent authorities' assessment will be guided by the SREP under Article 97 of Directive 2013/36/EU and in particular the technical criteria for the supervisory review and evaluation of exposure to and management of concentration risk by institutions under Article 98 of the same directive. Where it is deemed appropriate, consideration shall be given to the assignment of potential Pillar 2 requirements on specific institutions and, where necessary, competent authorities may also impose additional requirements under Article 104 of Directive 2013/36/EU where the risks arising from excessive exposures to shadow banking entities are not appropriately mitigated. The guidelines aim to provide a more structured basis for supervisors to make such Pillar 2 judgements within the supervisory review process in relation to exposures to shadow banking entities.

38. The combination of the chosen approach within the guidelines with the parallel option for supervisors to apply existing Pillar 2 measures in certain cases will allow the right balance to be found between allowing institutions to set their risk appetite for exposures to shadow banking entities and ensuring that their exposure does not result in excessive risk to the financial system.

3. Guidelines

EBA/GL/20XX/XX

DD Month YYYY

Guidelines

Limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[25]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/201x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation (EU) No 1093/2010.

[25] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter

5. These guidelines specify the methodology that should be used by institutions, as part of their internal processes and policies, for addressing and managing concentration risk arising from exposures to shadow banking entities. In particular, these guidelines specify criteria for setting an appropriate aggregate limit on exposures to shadow banking entities which carry out banking activities outside a regulated framework, as well as individual limits on exposures to such entities.

Scope of application

6. These guidelines fulfil the mandate given to the EBA under Article 395(2) of Regulation (EU) No 575/2013[26].

7. These guidelines build in particular on Articles 73 and 74 of Directive 2013/36/EU[27], which require institutions to have sound, effective and comprehensive strategies and processes to assess and maintain on an ongoing basis the amounts, types and distribution of internal capital that they consider adequate to cover the nature and level of the risks to which they are or might be exposed, as well as effective processes to identify, manage, monitor and report such risks and adequate internal control mechanisms; and Articles 97 and 103 of Directive 2013/36/EU, which establish that competent authorities must review the arrangements, strategies, processes and mechanisms implemented by institutions to comply with Regulation (EU) No 575/2013 and Directive 2013/36/EU, and evaluate the risks to which the institutions are or might be exposed, and that they may apply the supervisory review and evaluation process (SREP) to institutions which are or might be exposed to similar risks or pose similar risks to the financial system.

8. These guidelines apply to exposures to shadow banking entities as defined below.

9. These guidelines apply to institutions to which Part Four of Regulation (EU) No 575/2013 (Large Exposures) applies, in accordance with the level of application set out in Part I, Title II, of that Regulation.

[26] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) no 648/2012 (OJ L 321, 30.11.2013, p. 6).

[27] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

Addressees

10. These guidelines are addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010 and to financial institutions as defined in Article 4(1) of Regulation No 1093/2010.

Definitions

11. Unless otherwise specified, terms used and defined in Regulation (EU) No 575/2013 and Directive 2013/36/EU have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Credit intermediation activities	Bank-like activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar activities. These activities include at least those listed in the following points of Annex 1 of Directive 2013/36/EU: points 1 to 3, 6 to 8, and 10.
Exposures to shadow banking entities	Exposures to individual shadow banking entities pursuant to Part Four of Regulation (EU) No 575/2013 with an exposure value, after taking into account the effect of the credit risk mitigation in accordance with Articles 399 to 403 and exemptions in accordance with Articles 400 and 493(3) of that Regulation, equal to or in excess of 0.25% of the institution's eligible capital as defined in Article 4(1)(71) of Regulation (EU) No 575/2013.
Shadow banking entities	Undertakings that carry out one or more credit intermediation activities and that are not excluded undertakings.
Excluded undertakings	(1) undertakings included in consolidated supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013. (2) undertakings which are supervised on a consolidated basis by a third country competent authority pursuant to the law of a third country

which applies prudential and supervisory requirements that are at least equivalent to those applied in the Union.

(3) undertakings which are not within the scope of points (1) and (2) but which are:

(a) credit institutions;(b) investment firms;

(c) third country credit institutions if the third country applies prudential and supervisory requirements to that institution that are at least equivalent to those applied in the Union;

(d) recognised third country investment firms;

(e) entities which are financial institutions authorised and supervised by the competent authorities or third country competent authorities and subject to prudential requirements comparable to those applied to institutions in terms of robustness where the institution's exposure(s) to the entity concerned is treated as an exposure to an institution pursuant to Article 119(5) of Regulation (EU) No 575/2013;

(f) entities referred to in points (2) to (23) of Article 2(5) of Directive 2013/36/EU;

(g) entities referred to in Article 9(2) of Directive 2013/36/EU;

(h) insurance holding companies, insurance undertakings, reinsurance undertakings and third country insurance undertakings and third-country reinsurance undertakings where the supervisory regime of the third country concerned is deemed equivalent;

(i) undertakings excluded from the scope of Directive 2009/138/EC [28] in accordance with

[28] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II) (recast) (OJ L 335, 17.12.2009, p. 1).

Article 4 of that Directive;

(j) institutions for occupational retirement provision within the meaning of point (a) of Article 6 of Directive 2003/41/EC[29] or subject to prudential and supervisory requirements comparable to those applied to institutions within the meaning of point (a) of Article 6 of Directive 2003/41/EC in terms of robustness;

(k) undertakings for collective investment:

(i) within the meaning of Article 1 of Directive 2009/65/EC[30];

(ii) established in third countries where they are authorised under laws which provide that they are subject to supervision considered to be equivalent to that laid down in Directive 2009/65/EC;

(iii) within the meaning of Article 4(1)(a) of Directive 2011/61/EU[31] with the exception of:

- undertakings employing leverage on a substantial basis according to Article 111(1) of Commission Delegated Regulation (EU) 231/2013 [32] and/or
- undertakings which are allowed

[29] Directive 2003/41/EC of the European Parliament and of the Council of 3 June 2003 on the activities and supervision of institutions for occupational retirement provision (OJ L 235, 23.9.2003, p. 10).

[30] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast) (OJ L 302, 17.11.2009, p. 32).

[31] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

[32] Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision (OJ L 83, 22.3.2013, p. 1).

to originate loans or purchase third party lending exposures onto their balance-sheet pursuant to the relevant fund rules or instruments of incorporation;

(iv) which are authorised as 'European long-term investment funds' in accordance with Regulation (EU) 2015/760[33];

(v) within the meaning of Article 3 (1)(b) of Regulation (EU) 346/2013[34] ('qualifying social entrepreneurship funds');

(vi) within the meaning of Article 3(b) of Regulation (EU) 345/2013[35] ('qualifying venture capital funds').

except undertakings that invest in financial assets with a residual maturity not exceeding two years (short-term assets) and have as distinct or cumulative objectives offering returns in line with money market rates or preserving the value of the investment (money market funds);

(l) central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012[36] established in the EU and third country CCPs recognised by ESMA pursuant to

[33] Regulation (EU) 2015/760 of the European Parliament and of the Council of 29 April 2015 on European long-term investment funds (OJ L 123, 19.5.2015, p. 98).

[34] Regulation (EU) No 346/2013 of the European Parliament and of the Council of 17 April 2013 on European social entrepreneurship funds (OJ L 115, 25.4.2013, p. 18).

[35] Regulation (EU) No 345/2013 of the European Parliament and of the Council of 17 April 2013 on European venture capital funds (OJ L 115, 25.4.2013, p. 1).

[36] Regulation (EU) 648/2012 of European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

Article 25 of that Regulation;

(m) electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC[37];

(n) payment institutions as defined in point (4) of Article 4 of Directive 2007/64/EC[38];

(o) entities the principal activity of which is to carry out credit intermediation activities for their parent undertakings, for their subsidiaries or for other subsidiaries of their parent undertakings;

(p) resolution authorities, asset management vehicles and bridge institutions as defined in points (18), (56) and (59) of Article 2(1) of Directive 2014/59/EU[39] and entities wholly or partially owned by one or more public authorities established prior to the 1 January 2016 for the purpose of receiving and holding some or all of the assets, rights and liabilities of one or more institutions in order to preserve or restore the viability, liquidity or solvency of an institution or to stabilise the financial market.

[37] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

[38] Directive 2007/64/EC of the European Parliament and of the Council of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

[39] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU and Regulations (EU) No 1093/2010 and (EU) No 648/2012 of the European Parliament and of the Council (OJ L 173, 12.6.2014, p.190).

3. Implementation

Date of application

12. These guidelines apply from 01.01.2017.

4. Requirements regarding limits to exposures to shadow banking entities

13. Institutions should comply with the general principles referred to in this section, as well as set limits as referred to under Section 5, as applicable.

Effective processes and control mechanisms

14. Institutions should:

    a. Identify their individual exposures to shadow banking entities, all potential risks to the institution arising from those exposures, and the potential impact of those risks.

    b. Set out an internal framework for the identification, management, control and mitigation of the risks outlined in point a). This framework should include clearly defined analyses to be performed by risk officers regarding the business of a shadow banking entity to which an exposure arises, the potential risks to the institution and the likelihood of contagion stemming from these risks to the entity. Those analyses should be performed under the supervision of the credit risk committee, which should be duly informed of the results.

    c. Ensure that risks outlined in letter a) are adequately taken into account within the institution's Internal Capital Adequacy Assessment (ICAAP) and capital planning.

    d. Based on the assessment conducted under letter a), set the institution's risk tolerance/risk appetite for exposures to shadow banking entities.

    e. Implement a robust process for determining interconnectedness between shadow banking entities, and between shadow banking entities and the institution. This process should in particular address situations where interconnectedness cannot be determined, and set out appropriate mitigation techniques to address potential risks stemming from this uncertainty.

    f. Have effective procedures and reporting processes to the management body regarding exposures to shadow banking entities within the institution's overall risk management framework.

    g. Implement appropriate action plans in the event of a breach of the limits set by the institution in accordance with Section 5.

Oversight by the management body of the institutions

15. When overseeing the application of the principles referred to above as well as the application of limits set out in accordance with the principal approach in Section 5, the institution's management body should, on a regular predetermined basis:

    a. review and approve the institution's risk appetite to exposures to shadow banking entities and the aggregate and individual limits set in line with Section 5;

    b. review and approve the risk management process to manage exposures to shadow banking entities, including analysis of risks arising from those exposures, risk mitigation techniques and potential impact on the institution under stressed scenarios;

    c. review the institution's exposures to shadow banking entities (on an aggregate and individual basis) as a percentage of total exposures and expected and incurred losses;

    d. ensure the setting of the limits referred to in these guidelines is documented, including any changes to them.

16. The institution's management body may delegate the reviews set out in paragraph 15 a) to d) to senior management.

5. Principal approach for setting limits to exposures to shadow banking entities

Setting an aggregate limit on exposures to shadow banking entities

17. Institutions should set an aggregate limit to their exposures to shadow banking entities relative to their eligible capital.

18. When setting an aggregate limit to exposures to shadow banking entities, each institution should take into account:

    a. its business model, risk management framework as outlined in paragraph 14b), and risk appetite as outlined in paragraph 14d);

    b. the size of its current exposures to shadow banking entities relative to its total exposures and relative to its total exposure to regulated financial sector entities;

    c. interconnectedness as outlined in paragraph 14e).

Setting individual limits on exposures to shadow banking entities

19. Independently of the aggregate limit, and in addition to it, institutions should set tighter limits on their individual exposures to shadow banking entities. When setting those limits, as part of their internal assessment process, the institutions should take into account:

    a. the regulatory status of the shadow banking entity, in particular whether it is subject to any type of prudential or supervisory requirements;

    b. the financial situation of the shadow banking entity including, but not limited to, its capital position, leverage and liquidity position;

    c. information available about the portfolio of the shadow banking entity, in particular non-performing loans;

    d. available evidence about the adequacy of the credit analysis performed by the shadow banking entity on its portfolio, if applicable;

    e. whether the shadow banking entity will be vulnerable to asset price or credit quality volatility;

    f. concentration of credit intermediation activities relative to other business activities of the shadow banking entity;

    g. interconnectedness as outlined in paragraph 14 e);

    h. any other relevant factors identified by the institution under paragraph 14 a).

6. Fallback approach

20. If institutions are not able to apply the principal approach as set out in Section 5, their aggregate exposures to shadow banking entities should be subject to the limits on large exposures in accordance with Article 395 of Regulation (EU) No 575/2013 (including the use of Article 395(5) of the same Regulation) ('the fallback approach').

21. The fallback approach should be applied in the following way:

    a) If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4, they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).

    b) If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management body as set out in Section 4, but cannot gather sufficient information to enable them to set out appropriate limits as set out in Section 5, they should only apply the fallback approach to the exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach as set out in Section 5 should be applied to the remaining exposures to shadow banking entities.

4. Accompanying documents

4.1 Cost-Benefit Analysis/Impact Assessment[40]

4.1.1 Problem identification

The interconnectedness between the (regulated) banking sector and shadow banking entities and the specific risks posed by shadow banking entities to the stability of the financial system provide the motivation for action to be taken with regard to institutions' exposures to shadow banking entities.

Under the current regulatory regime, institutions' exposures to shadow banking entities are already subject to limits under the general framework for large exposures. However, the general framework for large exposures could be supplemented by provisions that would be specific to the monitoring and limiting of exposures to shadow banking entities, given the risks they might entail. To set such a framework, a set of decisions must be made regarding the scope of the application of the guidelines (in particular the definition of shadow banking entities) and the limits to be set.

4.1.2 Policy objectives

The present guidelines are intended to fulfil the regulatory objectives of (a) mitigating microprudential risk (i.e. risks posed to institutions as a result of their exposures to shadow banking entities), (b) mitigating macroprudential risks (e.g. financial stability) and (c) mitigating regulatory arbitrage risks (i.e. between the regulated and unregulated parts of the financial system). To achieve the regulatory objectives, the guidelines target specific and operational objectives. In particular, the guidelines aim to specify the scope of their application (specific objective), the definition of shadow banking entities (operational objective to meet the specific objective of the scope of application) and the types of limits which might be set (specific objective).

The legal mandate in Article 395(2) of Regulation (EU) No 575/2013 requires the EBA to issue guidelines to set appropriate aggregate limits to shadow banking exposures or tighter individual limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework, taking into account any material detrimental impact on the provision of credit to the real economy or on the stability of financial markets.

[40] The analysis in this section is partly based on information collected in a dedicated exercise and presented in more detail in the EBA Report on institutions' exposures to shadow banking entities (2015).

4.1.3 Options considered

First set of options (specific): scope of application/definition of shadow banking entities

The legal mandate requires the EBA to set limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework.

As a starting point, the EBA considers that 'banking activities' should be interpreted as activities involving maturity transformation, liquidity transformation, leverage, credit risk transfer or similar credit intermediation activities. To provide guidance to institutions the EBA suggests that these activities include at least those listed in points 1 to 3, 6 to 8 and 10 of Annex 1 of Directive 2013/36/EU. This is consistent with the approach adopted in international (in particular FSB) and other European contexts.

As for the interpretation of 'regulated framework', two key elements were considered: (i) the inclusion in prudential consolidation and supervision and (ii) specific solo prudential and conduct regulatory frameworks.

First, as regards the treatment of ***entities within the scope of prudential consolidation*** the following options were considered:

a. **Option 1.1:** Entities which are subject to prudential supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013 should be outside the definition of shadow banking entities only if they are also subject to solo prudential requirements which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU.

b. **Option 1.2:** Entities which are subject to prudential supervision on the basis of the consolidated situation of an institution as defined in Article 4(1)(47) of Regulation (EU) No 575/2013 should be outside the definition of shadow banking entities regardless of whether they are subject to solo prudential requirements which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU.

Preferred option: Option 1.2 is preferable, as any such entities carrying out credit intermediation activities would be subject to prudential requirements at the consolidated level as a result of prudential consolidation, thereby mitigating any risks posed by the bank-like activities carried out by those entities. Given this, these entities should not be regarded as being 'outside a regulated framework' and therefore should be carved out from the definition of shadow banking entities.

Second, for those ***entities that are not subject to prudential consolidation***, the EBA considered different types of regulatory frameworks. In particular, two options were considered:

a. **Option 2.1:** Institutions subject to third country prudential and supervisory requirements or other Union or national prudential frameworks, which are at least equivalent to Regulation (EU) No 575/2013 and Directive 2013/36/EU should be carved out from the definition of shadow banking entities.

b. **Option 2.2:** Entities subject to any regulatory framework (of a prudential or conduct nature) under Union law or equivalent third country or national law for institutions and other regulated entities should be carved out from the definition of shadow banking entities.

Preferred option: Having regard to the objectives identified in the section above, the focus of the policy debate on shadow banking in Union and international contexts, the need for EBA to act in a manner that is consistent and coherent with Union initiatives in the field of financial regulation, and the need for EBA to adopt a risk-based proportionate approach to regulation, the EBA considers that Option 2.1 is the only reasonable approach to interpretation for the purposes of the guidelines. Under that approach, such a 'regulated framework' is understood as a robust prudential regulation framework where credit, liquidity, leverage and other risks are adequately addressed.

The approach under Option 2.2, on the other hand, would exclude entities that are, for example, subject to a light touch or non-prudential regime which may fail to mitigate effectively risks posed by the carrying out of credit intermediation by the entity concerned.

The proposed approach, in contrast, would focus on entities that are not subject to an appropriate prudential framework, thereby concentrating on those entities that pose the greatest risks in terms of both the direct exposures institutions face and, more widely, the incentives for credit intermediation to be carried out outside the regulated framework.

According to the results of the dedicated data collection, only slightly more than 10% of the exposure amounts are to entities which are known to be supervised on a consolidated level in the Union or in a third country with an at least equivalent prudential regime. For almost 90% of the exposure amounts, the type of supervision of the counterparty is not known or not further specified. From a prudential perspective, this result justifies the option chosen above, as only a minor proportion of the exposure amounts is known to be supervised on a consolidated level and can consequently be reasonably carved out from the scope of application of these guidelines.

Turning specifically to the treatment of funds, these tend to engage in maturity and liquidity transformation and are generally regarded as outside the traditional banking sector. Therefore, *prima facie*, they should be within the scope of the definition of shadow banking entity. However, some funds are regulated pursuant to prudential frameworks similar to those applied to credit institutions and investment firms and should therefore be excluded from the scope of the guidelines. Based on the results of the data collection, the proportion of amounts of exposures (after taking into account credit risk mitigation and exemptions) to MMFs (UCITS and others) is rather small (< 5% of total exposure amounts). Around one quarter of the exposure amounts is to (non-MMF) investment funds, out of which one fifth is to hedge funds.

Second set of options (specific): establishment of limits

After assessing the objectives of the limits to be developed and the concerns to be addressed, EBA has identified three possible policy options (see 3.1 to 3.3 below).

a) **Option 3.1**: Explicit appropriate aggregate limits or tighter individual limits on exposures to shadow banking entities under Pillar 1

Setting tighter individual limits (i.e. an exposure limit lower than the large exposure limit of 25% of an institution's eligible capital after taking into account the effect of credit risk mitigation measures) or appropriate aggregated limits on exposures to individual shadow banking entities would be a very direct way to limit the regulated banking sector's exposures to shadow banking entities. When setting individual limits, different types of shadow banking entities, activities or instruments could be considered.

Given that any regulatory proposal about quantitative limits on exposures to shadow banking entities needs to be based on a thorough impact analysis, the EBA finds it premature to set out limits to individual or aggregate exposures to shadow banking entities. Simultaneously with issuing these guidelines, EBA is publishing an in-depth report to inform the Commission on European credit institutions' and investment firms' exposures to shadow banking entities. Based on that analysis, the co-legislators may decide on any harder limits in accordance with Article 395(2) of the CRR, after having assessed the appropriateness and impact of regulatory measures.

b) **Option 3.2**: Individual limits on exposures to shadow banking entities to be set by institutions

To the extent that shadow banking entities carry out banking activities, such as maturity and liquidity transformation, which are inherently risky, exposures to such entities may therefore also be inherently risky - and thus specific limits for individual and aggregate exposures are warranted (see further reasoning in section 2.*1.4, Rationale for limiting institutions' exposures to shadow banking entities*).

This approach could be understood as forming part of the Pillar 2 framework. It should be noted that concentration risk is clearly identified as a core part of the Supervisory Review Process within the Capital Requirement Directive.[41] Where a concentration risk to shadow banking entities was identified, then a capital add-on, or additional obligation on a bank's funding/liquidity structure, may be warranted.[42]

[41] See Directive 2013/36/EU – Section III, Article 98(1)(b).

[42] It should be noted that, in the Basel Capital Framework (and the CRD), concentration risk is not fully addressed in the context of Pillar 1. For credit risk it is assumed that IRB portfolios are perfectly diversified. Any resultant underestimation of risk should be corrected by addressing the concentration risk and allocating capital, where necessary. For details see the EBA guidelines on concentration risk: https://www.eba.europa.eu/documents/10180/16094/Concentration.pdf.

c) **Option 3.3**: Aggregate limits on exposures to shadow banking entities to be set by the institutions

The interconnectedness between the shadow banking and the regulated banking sector, plus the tendency of shadow banking entities to engage in excessively leveraged or otherwise risky activities, calls for management of exposures not only to individual shadow banking entities, but also to the shadow banking sector in its entirety.

Institutions may have an incentive to shift activities to the shadow banking sector in response to more stringent capital requirement. Also, periods of low real interest rates may fuel such a tendency as demand from institutional cash pools for alternative investment opportunities grows and the 'search for yield' phenomenon accelerates funds into the shadow banking sector. An overall backstop limit, together with improved identification of large exposures connected to the shadow banking sector, would help safeguard the regulated banking sector, preventing it from overly fuelling the growth of the unregulated shadow banking sector (thus getting overly interlinked and exposed).

The EBA sees that an aggregate limit to the shadow banking sector will result in a net benefit to the economy. From a macroprudential perspective, this approach should ensure that the shadow banking sector remains able to provide credit to the real economy without creating excessive risks to financial stability (including spillover risk). The institutions would set their aggregate limit to the aggregate of shadow banking entities, in the same way as described in Option 3.2.

If the approach under Options 3.2 and 3.3 ('the principal approach') cannot be applied, a 'fallback approach' would be applied, whereby a specific limit would be applied for the aggregate exposures to shadow banking entities. The report on institutions' exposures to shadow banking entities shows the distribution of institutions into different clusters by their exposure to the shadow banking sector. The following technical specifications are considered fallback solutions:

Option 3.3.a: If institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management board, regardless of whether they can gather sufficient information about their individual exposures they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities).

Option 3.3.b: If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board, but cannot gather sufficient information regarding one or more individual exposures, they should apply the fallback approach to all their exposures to shadow banking entities (i.e. the sum of all their exposures to shadow banking entities), regardless of whether the institutions are able to gather sufficient information on some exposures.

Option 3.3.c: If institutions can meet the requirements regarding effective processes and control mechanisms or oversight by their management board, but cannot gather sufficient information regarding one or more individual exposures, they should only apply the fallback approach to the

exposures to shadow banking entities for which the institutions are not able to gather sufficient information. The principal approach should be applied to the remaining exposures to shadow banking entities.

Preferred options: After deliberating all pros and cons from a prudential perspective and having regard to the feedback received during the public consultation, the EBA proposes to combine Options 3.2 and 3.3. Institutions should both set an aggregate limit to their exposure to the shadow banking entities and also set tighter limits to individual exposures to shadow banking entities. In addition, institutions unable to implement effective processes and control mechanisms or to ensure oversight by their management board should apply the fallback approach to all their exposures (Option 3.3a). However, if institutions can meet these requirements and can gather relevant information about one or more individual counterparties from the shadow banking sector, this would be recognised and the fallback approach would apply only to the exposures for which the institution has not been able to collect sufficient information (Option 3.3c).

In addition, for the purposes of the application of the guideline, institutions could either:

a) **Option 4.1**: consider only exposures, after taking into account credit risk mitigation techniques and exemptions, with a value equal to or in excess of 0.25% of the institution's eligible capital; or

b) **Option 4.2**: consider all exposures to shadow banking entities.

Option 4.1 is consistent with other EBA products in the area of large exposures[43] and would significantly alleviate the burden for institutions and is therefore proposed as the preferred option. Although some caution needs to be exerted when interpreting the reported data, the EBA's dedicated analysis estimates that around 97% of the number of exposures reported by institutions in the sample are below this materiality threshold, which alleviates considerably the burden of compliance with the guidelines.

4.1.4 Cost-benefit analysis

The EBA conducted a comprehensive data collection to better understand the relevance and characteristics of institutions' exposures to shadow banking entities and also to support the development and policy choices of these guidelines. Based on that data collection, the costs for credit institutions, the credit provided to financial counterparties and the real economy and the benefits for the solvency of individual institutions and the stability of the financial system are estimated in a separate report. For the purpose of the Commission's assessment of the appropriateness of imposing regulatory limits, that report also contains a comprehensive analysis of institutions' exposures to shadow banking entities.

[43] EBA Final Draft Regulatory Technical Standards on the determination of the overall exposure to a client or a group of connected clients in respect of transactions with underlying assets under Art. 390(8) of Regulation (EU) No 575/2013.

Concerning the impact on the risk profile of credit institutions and investment firms, the results of the dedicated data analysis confirm that the number of exposures above common large exposure thresholds (e.g. 10% for reporting requirements, 25% for quantitative restrictions) is rather small. Relative to their eligible capital, average individual exposures are significantly higher (a multiple) for small and/or domestic institutions (Group 2 banks) and investment firms than for large and internationally active banks (Group 1). These guidelines should contribute to improved risk management and more comprehensive counterparty information collection. Requirements for individual and aggregate limits can be reasonably expected to contribute to less concentration risk towards shadow banking entities/the shadow banking sector for both Group 1 and Group 2 banks as well as investment firms. The majority of institutions' qualitative responses to the data collection associate exposures to shadow banking entities with above-average risk weights. Around a quarter of institutions associate higher revenues with shadow banking exposures and estimate the overall impact of their replacement by other exposures to be rather costly in profitability terms.

The potential detrimental impact on the provision of credit to the real economy in the EU is expected to be small (to medium) and carefully managed by the design of these guidelines. The results of the dedicated data collection show that around half of the amount of funds provided by European institutions is to counterparties resident outside the EU. It is rather unlikely that those funds would be finally destined for financing the real economy in the EU. Further, a certain proportion of those funds is provided to types of counterparty which are far less likely to focus on the direct provision of credit to the real economy. Thus the potential detrimental impact of limiting exposures to hedge funds, MMFs or broker-dealers is expected to be rather small. Lastly, the restriction of the application of these guidelines to exposure values after taking into account credit risk mitigation and exemptions, exposures to counterparties not (known to be) equivalently supervised at consolidated level, the qualitative principle-oriented approach of these guidelines and the application of a materiality threshold have all been designed to mitigate any potential detriment to the provision of credit to the real economy.

The direct and indirect beneficial impact on the stability and orderly functioning of financial markets in the EU is expected to be medium to high. Firstly, the largest part of European institutions' exposures to shadow banking entities is in the portfolio of Group 1 banks. Those, on average, exhibit higher exposures to the shadow banking sector in its entirety. Limiting concentrated exposures of institutions which are closer to being systemically important (because of their size and interconnectedness) to a potentially risky sector has benefits for financial stability. Similarly, certain types of counterparty entities are commonly perceived as carrying out risky activities (e.g. reliance on leverage, use of complex financial instruments) and being subject to relatively light prudential regulation (e.g. hedge funds). Limiting institutions' exposures to those counterparties which are also commonly perceived to behave in a correlated manner (e.g. invested in similar markets) can contribute to dampening procyclicality and systemic risk. Finally, the indirect approach of shadow banking regulation via tighter regulation of institutions' interaction with shadow banking entities can constitute a backstop to regulatory arbitrage. In summary, these guidelines are assumed to efficiently contribute to achieving the objectives stated above, while allowing for further regulatory intervention if considered appropriate.

4.2 Views of the Banking Stakeholder Group (BSG)

General comments

The consultation paper is an addition to other existing measures (such as SFT rules, haircut and reporting rules, etc.) that are designed to reduce systemic risk migration from the (largely unregulated) shadow banking sector to the highly regulated banking sector.

It is widely accepted that shadow banks of various sorts played an important role in the recent global banking crisis and that there were flaws in the way that such institutions operated and the links between the banking and shadow banking sectors. However, many of these flaws have since vanished as markets and institutions have reacted.

As a point of perspective, we also note that regulated banks are already subject to 'large exposure' rules irrespective of whether this relates to positions vis-à-vis banks or shadow banks. Furthermore, general capital requirements have been tightened up. Overall, these measures are likely to reduce the activity of banks vis-à-vis non-banks in general and shadow banks in particular.

The shadow banking landscape includes a heterogeneous set of institutions which cover a wide range of business activities and different business structures, and its size and functions can vary significantly between countries and markets. The shadow banking sector has a function in parallel with, and as a complement to, the banking system but on the other hand can create complexity and systemic risks. In addition, there is a risk of an undesirable risk transfer from the directly regulated sector to the shadow banking sector. The risk related to the shadow banking sector can to some extent be mitigated through indirect regulation, for example limitations for institutions to securitized assets, or as direct regulation towards shadow banking entities as example through AIFMD. Even if the indirect approach might have an impact in mitigating the risk in some areas, the view of BSG is that a more robust long term solution includes a regulation covering the shadow banking entities and its intermediation activities.

Before considering the specific questions raised in the consultation paper, we emphasise three general concerns. Firstly, there is a potential danger that the overall regulatory regime that is applied to regulated banks may not be as sufficiently competitively neutral as between institutions conducting essentially similar business and that this may unnecessarily distort competition between the regulated banking sector and the less-regulated institutions in the shadow banking sector.

A second concern is that regulatory agencies and national authorities should have a common definition of what is meant by 'shadow banks', and that regulation and supervision of the relationship between banks and shadow banks should be applied consistently between countries. This also raises issues of competitive neutrality between different national regulatory regimes.

Thirdly, the proposed rules outlined in the consultation paper may have the unintended consequence of undermining the fluidity of securitisation schemes that are currently proposed under the Capital Market Union: this may again produce regulatory inconsistencies.

Replies to questions

Q1. Do you agree with the approach the EBA has proposed for the purposes of defining shadow banking entities? In particular, do you consider that this approach is workable in practice? If not, please explain why and present possible alternatives.

In the FSB's 2014 Global Shadow Banking Monitoring Report, the shadow banking sector is defined as credit intermediation involving entities and activities outside the regular banking system or, as other market participants prefer, as 'market based activity'. This is a very broad definition and, in addition, the term carries a negative image. However, often this activity with non-bank financial institutions is carried out with institutions which are highly regulated, such as UCITS or insurance companies. As the consultation paper proposes increased control mechanisms towards shadow banking entities, a clear and operational definition is of great importance.

In this context we again emphasise the need for a common global definition of shadow banking.

The approach of defining entities that is out of scope for the definition of shadow banking is relevant and easy to adopt. In addition, the exposures towards UCITS are to a large extent already restricted by limits contained in the CRR. The most relevant approach for defining shadow banking entities seems to be by reference to the activities performed. Some of these are listed in the proposal with reference to CRD, annex 1. There is, nevertheless, considerable room for different translation of entities and activities in scope and the definitions still involve a high degree of subjectivity. Exposures to funds that are not considered as excluded undertakings should be possible to be treated by a look through principle where possible. It is also unclear how the exposure towards entities with mixed business lines should be treated in this context. As an example, should the total exposure towards an entity with some kind of shadow banking activity be considered as shadow banking in total when defining limits and interconnectedness?

The definition is broad and may generate a high number of 'positives', which could lead to an additional operational risk and disproportionate burden in terms of policies and control mechanisms, given that there would likely be only a relatively small overall risk reduction in the banking sector.

The view of the BSG is that the threshold of 0.25% is too low and the process of maintaining, monitoring and reporting these can be excessively administratively burdensome and disproportionate, considering turnover in portfolios and interconnectedness but also considering the fallback approach option 1 or option 2.

Q2. Do you agree with the approach the EBA has proposed for the purposes of establishing effective processes and control mechanisms? If not, please explain why and present possible alternatives.

The process will require specific instructions and monitoring and reporting requirements that are directly related to entities defined as shadow banking. Risk related to concentration and interconnectedness and specific risk towards specific entities is already an integrated part of the credit risk monitoring entity within most institutions and the need to set specific restrictions, at an institutional level towards a broad category of companies sorted into the category shadow banking, could be questioned. The definition of shadow banking entities includes intermediate activities, but in many cases this may be the only common denominator.

The proposed specific requirement for shadow banking entities related to Pillar 2 can be questioned, since the Pillar 2 requirements are already defined and in use already.

Q3. Do you agree with the approach the EBA has proposed for the purposes of establishing appropriate oversight arrangements? If not, please explain why and present possible alternatives.

It could be questioned if there is a need to have a specific process for exposures defined as being within the shadow banking definition. Risks, limits and risk appetite are an integral part of the credit risk monitoring and reporting process. However, we agree in principle with the arrangements.

Q4. Do you agree with the approaches the EBA has proposed for the purposes of establishing aggregate and individual limits? If not, please explain why and present possible alternatives.

An aggregated limit only has relevance if there is a defined interconnectedness between two or more entities in scope for the definition of shadow banking. There are potentially less combined risk and interconnectedness in exposures towards totally different shadow banking activities in different countries compared to some other interconnections which already should be considered following the large exposures regulation. Besides, indirect interconnectedness is difficult to assess in practice, for example if there are holdings by other institutions. With reference to no 18 of the consultation it is stated that the EBA is considering updating the 'Guidelines on the identification of groups of connected clients under Article 4, Para. 1, No 39 Regulation (EU) No 575/2013, including providing greater clarity on how institutions and special-purpose vehicles can be economically interdependent.'

The view of the BSG is that the review and updating of that guideline should be undertaken in parallel with the guideline on shadow banking. Furthermore, indirect interconnectedness is to some extent already addressed in the BCBS paper 'Supervisory framework for measuring and controlling large exposures', April 2014. Even though the Basel paper considers the identification of additional risk imposed by third parties by the structure the bank invests in (e.g. in the case of an originator, fund manager, liquidity provider or credit protection provider), there are remaining difficulties in identifying all those connections. Furthermore, the Basel paper remains vague in the case of structured finance products.

Q5. Do you agree with the fall back approach the EBA has proposed, including the cases in which it should apply? If not, please explain why and present possible alternatives. Do you think that Option 2 is preferable to Option 1 for the fall back approach? If so, why? In particular: Do you believe that Option 2 provides more incentives to gather information about exposures

than Option 1? Do you believe that Option 2 can be more conservative than Option 1? If so, when? Do you see some practical issues in implementing one option rather than the other?

The view of the BSG is that Option 2 is the preferred option, since the requirements for the main part of exposures are fulfilled and should not be affected by a small number of exposures where the criteria are not met. It would be to presume a very close linkage between normally rather heterogeneous entities that are treated as directly connected. The most conservative outcome of the different options should not be the main reason for preference and could basically be affected by just one minor exposure. However, a technical fallback is not necessarily the only approach to address shortcomings, as in the SPREP and by capital add-on.

4.3 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the guidelines contained in this paper.

The consultation period lasted for 3 months and ended on 19 June 2015. 57 responses were received, of which 48 were published on the EBA website, including the opinion of the BSG.

This paper presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases, several industry bodies made similar comments or the same body repeated its comments in response to different questions. In such cases, the comments, and the EBA's analysis, are included in the section of this paper where the EBA considers them most appropriate.

Changes to the guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

Most respondents focused their feedback on the proposed scope of the guidelines and the proposed definition for 'shadow banking entities' and argued for further exemptions. The EBA has carefully considered this feedback and amended the definition of 'excluded entities' to consider additional exceptions, which were intended but not clearly set out in the consultation paper, and has also revised its policy decisions regarding the treatment of certain funds.

Some respondents were critical about the fallback approach, in particular Option 1 in the consultation paper. The EBA has considered this feedback and redesigned the fallback approach along the lines of Option 2 in the consultation paper. The data collection has provided useful input to confirm the calibration of the fallback approach.

Summary of responses to the consultation and the EBA's analysis

Summary of responses received	EBA analysis	Amendments to the proposals
General comments		
The EBA's mandate expressly requires that 'international level' developments on shadow banking should be taken into account in the development of these guidelines. Proper coordination has to be ensured with existing international work on shadow banking before setting a definition (e.g. work undertaken by the Basel Committee on Banking supervision, the Financial Stability Board, ESMA or the G20). There is a need for development of a fundamental and robust level 1 regulation designed for shadow banking entities.	The EBA has given due consideration to on-going work in the area of shadow banking in the Union and other international fora. The EBA has also consulted the ESMA, the FSB, the European Commission services and the European Central Bank regarding the proposed definition of 'shadow banking entities' and has considered their feedback when finalising the guidelines. The EBA notes that the suggestion for regulating the shadow banking sector goes beyond the scope of the guidelines.	No amendment.
Responses to questions in Consultation Paper EBA/CP/2015/06		
Q1. Do you agree with the approach the EBA has proposed for the purposes of defining shadow banking entities? **In particular:** **Do you consider that this approach is workable in practice? If not, please explain why and present possible alternatives.** **Do you agree with the proposed approach to the exclusion of certain undertakings, including the approach to the treatment of funds? In particular, do you see any risks stemming from the exclusion of non-MMF UCITS given the size of the industry? If you do not agree with the**		

Summary of responses received	EBA analysis	Amendments to the proposals
proposed approach, please explain why not and present the rationale for the alternative approach(es) (e.g. on the basis of specific prudential requirements, redemption limits, maximum liquidity mismatch and leverage, etc.).		
Most respondents focused their feedback on the scope of the guidelines and the proposed definition of 'shadow banking entities'. **Definition of 'credit intermediation activities':** • **Portfolio management and advice** – regarding the definition of 'credit intermediation activities', feedback noted that 'credit intermediation activities' are not present while carrying out portfolio management and advice according to point 11 of Annex I of the CRD. Moreover, this activity is also regulated by the Markets in Financial Instruments Directive 2004/39/EC, by the UCITS Directive and, if undertaken by AIF managers, the AIFMD. • **Relation of bank-like activities and CRD/Annex I references -** some respondents also sought clarification of whether the four proposed bank-like activities for the identification of an activity as 'credit intermediation activities' are independent of the eight activities proposed by reference to Annex I of CRD IV. **Definition of 'excluded undertaking':** Broadly, respondents' view was that the proposed catalogue of excluded undertakings is too narrow, and does not take into account the wide diversity in underlying business models and activities that exists in practice. Various additional segments of the non-bank sector should be excluded from the definition of 'shadow banking entities'. Respondents	**Definition of 'credit intermediation activities'** *Portfolio management and advice:* On reflection, the EBA regards it as inappropriate to include this activity in the list of activities which institutions can consider automatically as 'credit intermediation activities', as it is not always the case that this activity will involve credit intermediation. Instead, the institution would need to carry out a case-by-case assessment of an entity's business (assuming that the entity concerned does not carry out one of the other activities listed in the definition of 'credit intermediation activities') in order to identify whether the entity is to be considered a 'shadow banking entity' for the purposes of the guidelines. *Relation of bank-like activities and CRD/Annex I references:* The referenced activities mentioned in Annex I of the CRD should be understood as examples	**Definition of 'credit intermediation activities'** *Portfolio management and advice:* The definition of 'credit intermediation activities' has been amended to omit the reference to point 11 of Annex I to the CRD (portfolio management and advice). *Relation of bank-like activities and CRD/Annex I*

Summary of responses received	EBA analysis	Amendments to the proposals
cited the existence of various regulatory frameworks that applied already to certain entities in the non-bank sector. Concerns on the impact of the proposed broad scope were expressed – including about the cost of financing to the real economy in some cases. A list of the entities that were put forward for exclusion by respondents (in addition to those identified in the EBA's proposed list of excluded undertakings) is provided below. Some respondents proposed that the EBA use the definition of 'unregulated financial entity' as set out in Article 142(1) point 5 of Regulation (EU) No 575/2013 (the CRR). • **Money market funds (MMFs)** – respondents noted that most MMFs in the EU (80% of the assets and 60% of the funds) operate under the rules of the UCITS Directive[44], with the remainder operating (since July 2013) under the rules of the AIFMD[45]. Respondents cited the following requirements as providing specific prudential controls: i) Run risk and/or liquidity problems are addressed by risk management, liquidity management requirements, gates and liquidity fees requirements as set out in Article 16 of the AIFMD and Section 4 of Regulation 231/2013[46], and/or	of credit intermediation activities. **Definition of 'excluded undertaking'** *MMFs:* The EBA notes the consultation feedback regarding MMFs. For the reasons given in the consultation paper the EBA considers that, at this stage, in particular pending the agreement of the European Commission's proposal for a regulation on MMFs[61], and noting the size of the funds (for instance, relative to other types of UCITS), it remains appropriate for MMFs to fall within the scope of the definition of 'shadow banking entity'. The EBA will keep the scope of the guidelines under review, in particular having regard to relevant regulatory	*references:* No amendment. **Definition of 'excluded undertaking'** *MMFs:* No amendment. *AIFs:* The definition of 'excluded undertaking', point K) has been amended.

[44] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

[45] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

[46] Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision.

Summary of responses received	EBA analysis	Amendments to the proposals
Directive 2010/43/EU [47], as well as more MMF-specific requirements by CESR guidelines 10-49 [48] and ESMA guidelines, which since 2010 have imposed strict limits in term of liquidity, risk and leverage on all MMFs in Europe and limit the use of derivatives. ii) Interconnectivity and spillovers are addressed by counterparty limits and risk management requirements as set out in Article 15 of AIFMD and Section 3 of Regulation 231/2013, the UCITS Directive and Directive 2010/43/EU. iii) Excessive leverage and procyclicality are addressed by limits on leverage and disclosure on leverage as set out in Articles 11, 22 and 112 of the AIFMD, the UCITS Directive, Directive 2010/43/EU and CESR guidelines 10-788[49], as well as more MMF-specific requirements by CESR guidelines 10-49 and ESMA guidelines 2014/110. iv) Opaqueness and complexity are addressed by the obligation	developments. *AIFs:* The EBA has considered the feedback received during the consultation period as well as input from ESMA and the European Commission. The EBA acknowledges that AIFs are regulated indirectly, as a result of requirements imposed on their asset managers under the AIFMD. However, the risks arising directly from the funds themselves are not mitigated in a satisfactory way from a prudential point of view. For example, while leverage is strictly limited for UCITS funds, a similar limitation does not apply to AIFs. Given this, the EBA is of the view that only AIFs with limited leverage could be considered to fall outside the definition of 'shadow banking entities'. Under the AIFMD, a	*Particular case of EuVECAs, EuSEFs and ELTIFs:* The definition of 'excluded undertaking', point K) has been amended to include these specific cases. *Transactions with underlying assets:* No amendment. *Securitisation*

[61] The Commission's proposal is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.

[47] Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company.

[48] CESR's Guidelines on a common definition of European money market funds (review).

[49] CESR's Guidelines on a common definition of European money market funds.

Summary of responses received	EBA analysis	Amendments to the proposals
to report to investors and regulators (i.e. national competent authorities, ESMA and the ESRB) and supervise managers, as set out by Articles 22, 23, 24, 26, and Annex IV of the AIFMD, and by Commission Regulation (EU) No 583/2010[50]. Specific existing arrangements under the CRR (e.g. increases in risk weights for institutions' exposures to the unregulated financial sector, higher capital requirements for banks' investments in the equity of funds), as well as the introduction of liquidity and funding requirements under Basel III (e.g. liquidity coverage ratio, net stable funding ratio) were also invoked to prove that institutions will be less susceptible to liquidity and funding risks arising. The proposed MMFs Regulation[51] was noted, which will soon add to the weight of regulation on this sector. Further, the importance of MMFs as a source of funding for governments, corporates and financial institutions was highlighted – with concerns raised on how the guidelines may affect MMFs' role in providing this finance. • **Alternative investment funds (AIFs)** – respondents noted that all non-UCITS investment funds are regulated under AIFMD – which applies similar or even identical requirements to UCITS in many areas, e.g. liquidity management requirements, counterparty limits, leverage restrictions and disclosure. Respondents cited the following	fund manager who manages an AIF which employs leverage must, on a regular basis, disclose to its investors any change to the maximum level of leverage permitted as well as any re-hypothecation rights or any guarantee granted under the leveraging arrangement and the total amount of leverage employed by the AIF. For an institution, it would thus be easy to identify which AIF counterparty is leveraged or not. In addition to this condition, only AIFs which are not allowed to originate loans or purchase third parties' lending exposures and add them to their balance sheets would be excluded from the definition of 'shadow banking entity'. *Particular case of EuVECAs, EuSEFs and ELTIFs:* Regarding the particular case of EuVECAs (European Venture Capital Funds), EuSEFs (European Social Entrepreneurship Funds) and ELTIFs (European Long Term Investment Funds), the EBA is of the view that since these funds are	*activity:* No amendment. *Factoring and leasing companies:* The definition of 'financial institution' has been amended to clarify that it is to be interpreted in line with Article 119(5) of the CRR. *Payment institutions and electronic money issuers:* The definition of

[50] Commission Regulation (EU) No 583/2010 of 1 July 2010 on key investor information and conditions to be met when providing key investor information or the prospectus in a durable medium other than paper or by means of a website.

[51] The Commission's proposal for the regulation is available here: http://ec.europa.eu/finance/investment/money-market-funds/index_en.htm.

Summary of responses received	EBA analysis	Amendments to the proposals
requirements as providing specific prudential controls: i) Run risk and/or liquidity problems are addressed by risk management, liquidity management requirements, gates and liquidity fees requirements as set out by Article 16 of the AIFMD, Section 4 of Regulation 231/2013 and the EVCA risk measurement guidelines[52]. ii) Interconnectivity and spillovers are addressed by counterparty limits and risk management requirements as set out by Article 15 of the AIFMD and Section 3 of Regulation 231/2013. iii) Excessive leverage and procyclicality are addressed by limits on leverage and disclosure on leverage as set out in Articles 11, 22 and 112 of the AIFMD. iv) Opaqueness and complexity are addressed by the obligation to report to investors, report frequently and in a granular way to regulators (i.e. national competent authorities, ESMA and the ESRB) and supervise managers, as set out by Articles 22, 23, 24, 26, and Annex IV of the AIFMD. It was stressed that supervisory reporting on a quarterly basis is mandatory for most AIFs and includes detailed information on portfolio composition, principal exposures and most	closed-ended vehicles that do not usually perform credit intermediation they should fall outside the definition of 'shadow banking entity' and be out of the scope of the guidelines. *Transactions with underlying assets:* The EBA notes that the guidelines apply in parallel with Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014. This delegated regulation addresses concerns related to the failure of a single counterparty or a group of connected counterparties and sets out conditions under which the transaction itself does not constitute an additional exposure and is not subject to a limit. The guidelines address a different set of concerns, as laid out in the background section, and require that any transaction is subject to a limit. *Securitisation activity:* The mere fact that a securitisation is compliant	'excluded undertaking' has been amended to include two new points dealing expressly with 'electronic money institutions' and 'payment institutions'. *Resolution authorities, bridge institutions and asset management vehicles and similar entities established for the purposes relating to the resolution of institutions:* The definition of 'excluded

[52] https://www.evca.eu/media/10083/EVCA-Risk-Measurement-Guidelines-January-2013.pdf

Summary of responses received	EBA analysis	Amendments to the proposals
significant counterparty concentrations, risk profile and liquidity management, which proves helpful for assessing the interconnectedness between institutions and other financial entities. Furthermore the AIFMD reporting has been developed with the specific aim of enabling supervisory authorities to effectively monitor systemic risks associated with AIF management. Specific reporting is due by AIFs that use significant leverage (commitment in excess of 3 for 1 of capital). v) An exchange of information on the potential systemic consequences of AIFM activity is ensured by Article 116 of the AIFMD. vi) The obligatory use of AIF depositaries means that legal and operational structures must be provided to prevent cash flows from being redirected, just as with UCITS. The proposed Securities and Financing Transactions Regulation[53], Solvency II, and the Banking Structural Reform Regulation[54] were cited as a further set of requirements that will soon add to the weight of regulation on AIFs and the interactions between credit institutions and AIFs.	with the 'Simple, transparent and standardised' (STS) requirements would not be sufficient to justify securitisation vehicles being 'excluded undertakings'. In fact, the STS requirements do not mitigate prudential risk as such. Nevertheless the institution could take into account the fact that a securitisation is compliant with STS requirements when setting up a limit to its individual exposure to such securitisation. *Factoring and leasing companies:* The feedback touches two different aspects. Firstly, the industry claims that there is low reliance on short-term funding amongst leasing companies. This point relates to the question whether the criteria of 'credit intermediation activity' are fulfilled or not (see above). The EBA notes in this regard that this statement needs to be taken into account while applying the guidelines. It does not request a modification of	undertaking' has been amended to include a new point for such entities. *Financial companies carrying out credit intermediation activities for group companies:* The definition of 'excluded undertaking' has been amended to include a new point (o) to cover entities which have as their principal activity

[53] The Commission's original proposal for the regulation is available here: http://ec.europa.eu/finance/general-policy/shadow-banking/index_en.htm#maincontentSec1.

[54] The Commission's original proposal for the regulation is available here: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CC0QFjAB&url=http%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FALL%2F%3Furi%3DCELEX%3A52014PC0043&ei=V6CSVYD_JcOX7Qan8JH4Cw&usg=AFQjCNHS6W7SrEYm95rX6F12fm86uF38RA&bvm=bv.96783405,d.ZGU.

Summary of responses received	EBA analysis	Amendments to the proposals
A number of bodies also stressed that the population of AIFs is very diverse – and that the draft guidelines risked applying an inappropriate 'one size fits all' approach that would ignore the divergent riskiness that different AIFs represent. In this same regard, some respondents suggested that only AIFs that employ substantial leverage (as defined in Article 111 of Regulation 213/2013) should be captured in the guidelines. The distinction that has been proposed between AIFs and UCITS was also questioned – as some respondents stated that AIFs are often not substantially different from UCITS in risk terms, or in terms of the prudential regime applied. Furthermore the treatment of non-UCITS (and MMFs) should be consistent throughout the large exposure framework, in particular considering Commission Delegated Act 1187/2014[55], which distinguishes funds solely based upon their added risk. Most respondents see no specific justification for not excluding from the scope of the term 'shadow banking entity' certain closed-ended and unleveraged AIFs, EuVECAs, EuSEFs and ELTIFs, as these provide useful and much-needed financing to EU businesses and economies. • **Transactions with underlying assets** – some respondents highlighted a risk of duplication in cases where institutions 'look through'[56] their	'credit intermediation activity'. Secondly, assuming that a specific leasing or factoring company exercises 'credit intermediation activity', these companies will fall within the definition of 'financial institution' according to point (e) of excluded undertakings. The EBA clarifies that the definition of 'financial institution' should be interpreted in line with Article 119(5) of the CRR (exposures to institutions). That is, where an institution's exposure to an entity (for instance a factoring or leasing company) is treated as an exposure to an institution pursuant to Article 119(5) of the CRR, because the entity is subject to a comparable prudential framework to that applicable to institutions in terms of robustness, the entity should be regarded as a 'financial institution' for the purposes of the guidelines. In such cases the entity shall not be treated as a 'shadow banking entity' for the purposes of the guidelines.	carrying out credit intermediation activities for their parent undertakings, for their subsidiaries or for other subsidiaries of their parent undertakings. **Consolidation** No amendment. **Equivalence of third country regimes** No amendment.

[55] Commission Delegated Regulation (EU) No 1187/2014 of 2 October 2014 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council as regards regulatory technical standards for determining the overall exposure to a client or a group of connected clients in respect of transactions with underlying assets.

[56] See Article 7 of Commission Delegated Regulation (EU) No 1187/2014 - banks can base their exposure for the purposes of the large exposures regime solely on the assets in the funds and do not have to include the funds themselves or their managers.

Summary of responses received	EBA analysis	Amendments to the proposals
exposures to investment funds in measuring their exposures for large exposures purposes. Where the look-through approach is used for measuring exposures to a fund (e.g. UCITs and AIFs), it was argued that additional exposure limits under the proposed guidelines are not necessary – and thus that the exposure to the fund should be excluded from the scope of the guidelines. • **Securitisation activity** – Related to the *Look-Through Approach*, some respondents noted that exposures to securitisations are also generally handled under this system – and thus that exposures arising in connection with securitisations should also be explicitly excluded from the scope of the guidelines. Additionally, some concerns were expressed that capturing securitisation exposures would run counter to the overall direction of policy at present, which is seeking ways to 'revitalise' securitisation markets. Such concerns applied also to special-purpose vehicles (SPVs) and conduits, which respondents argued should also be excluded from the guidelines. Traditional 'self-liquidating' securitisation activity, it was argued, does not involve material maturity transformation, as investors' rights to repayment arise from the cash generated by the underlying securitised assets. Given this, securitisation activity may not involve 'bank-like activity' and thus it should be made explicit that this situation is excluded from the definition of shadow banking for the purpose of these guidelines. Where securitisations meet the new requirements (to be finalised) for *simple, transparent, and standardised* securitisation, the above	*Payment institutions and e-money issuers:* The EBA agrees that, due to the Union frameworks applicable to such entities, the definition of 'excluded undertaking' should be clarified to make it clear that such entities are not to be treated as a 'shadow banking entity' for the purposes of the guidelines. The EBA also points out that this clarifies a pre-existing policy position. *Resolution authorities, bridge institutions and asset management vehicles and similar entities established for the purposes relating to the resolution of institutions:* The EBA agrees with the consultation feedback regarding the treatment of exposures to entities established for purposes relating to the resolution of institutions pursuant to Directive 2014/59/EU or for similar purposes as, broadly speaking, these entities are established in pursuance of public policy objectives relating to financial stability. Accordingly the EBA agrees that such entities should not fall within the scope of the definition of 'shadow banking	**Groups of connected clients** The definition of 'exposure to shadow banking entity' has been amended to clarify that these are exposures to individual entities.

Summary of responses received	EBA analysis	Amendments to the proposals
arguments for exclusion were felt to be stronger still. Additional relevant prudential requirements in relation to securitisation were also noted – including within the CRR, where specifics are laid out on minimum retention, the treatment of liquidity lines to SPVs and the risk weighting of credit exposures[57]. • **Factoring and leasing companies** – feedback from the industry noted that this sector is regulated under national law[58], and thus is subject to some prudential requirements that ensure risks are appropriately managed. Given this, some respondents advocated for the exclusion of this sector from the scope of the guidelines. Further, it was claimed that the activity in this sector is not generally 'banking-like' – and therefore it would not be appropriate for the sector to be labelled as 'shadow banking'. In particular, it is claimed that there is low reliance on short-term funding amongst these companies, that leverage is not a major feature of the markets they operate in and that they are generally transparent – e.g. via published accounts of parent companies. The statement by the Haut Conseil de Stabilité Financière	entity'. *Financial companies carrying out credit intermediation activities exclusively for group companies:* The EBA notes the consultation feedback regarding the treatment of entities which carry out credit intermediation activities exclusively (or as their main business) for non-financial sector group companies. The EBA agrees that such entities should not fall within the scope of the definition of 'shadow banking entity' as long as their principal activity is to carry out credit intermediation activities for other entities of their non-financial group and not for third parties. **Consolidation**	

[57] See Part 3, Chapter 5, and Part 5 of the CRR.

[58] For example, the feedback noted national regimes in (i) supervision by the German supervisory authority for financial services institutions and the Deutsche Bundesbank that are legally enabled by the German Banking Act to obtain a comprehensive assessment of the risk situation of any leasing company at any time, (ii) UK Financial Conduct Authority's regime regulating the consumer credit markets and (iii) authorisation and regulation by the French national competent authority.

Summary of responses received	EBA analysis	Amendments to the proposals
(HCSF) in its 2015 annual report that French financing companies do not constitute shadow banks was noted[59]. It was also suggested that it should be clarified that rental companies are not considered leasing companies. • **Payment institutions and electronic money institutions** – their exclusion should be clarified, as such institutions are regulated and authorised under the EU Payment Services Directive 2007/64 (PSD-1) and EU E-money Directive 2009/110, and also, if credit related to payment services is granted, under Article 16, paragraph 3, of the PSD-1. • **Public resolution agencies** ('Finanzmarktstabilisierungsfonds') – these institutions wind down risk exposures and non-strategic business lines from banking institutions in trouble. They are subject to German national legislation[60] and supervision by the German Federal Agency for Financial Market Stabilisation and the German Federal Financial Supervisory Authority. • **Finance companies relating to industrial groups** – concerns were expressed that the proposed approach would capture exposures to entities that carry out 'bank-like activities' only as a small part of their business, e.g. the treasury/liquidity management function of	The EBA's intention is to exclude entities which are subject to prudential consolidation (i.e. which form a group with an institution) and to which CRR/CRD requirements apply at the consolidated level. **Equivalence of third country regimes** The EBA notes the consultation feedback regarding the process for assessing the equivalence of third country regimes. The EBA notes that this is a cross-cutting issue relevant to the application of various provisions of the CRD/CRR which refer to entities subject to third country regimes comparable to those in the Union. Consistent with normal practices, it is for institutions to assess whether a third country regime is comparable. In so doing, institutions may have regard to relevant decisions, including the Commission's Decision of 12 December 2014 on the equivalence of the supervisory and regulatory requirements of certain third countries and territories for the purposes of the treatment of exposures	

[59] http://www.economie.gouv.fr/files/hcsf_rapport_annuel_062015.pdf

[60] Act on the Establishment of a Financial Market Stabilisation Fund (Finanzmarktstabilisierungsfonds Gesetz, FMStFG).

Summary of responses received	EBA analysis	Amendments to the proposals
corporates. It was considered disproportionate to capture the exposure within the guidelines, as such intragroup operations are industry standard practices and neither create additional risks for the group as a whole nor increase the interconnectedness with institutions and the financial system (and thus do not pose a systemic risk). EMIR exempts intragroup OTC derivative transactions from the clearing obligation and margining requirements for non-centrally cleared transactions as long as the clearing thresholds are not crossed. In the same way, Article 2(1)(b) of Directive 2014/65/EU (MiFID II) deliberately waives the application of its provisions in full with regard to investment services exclusively provided for parent undertakings, for subsidiaries or for other subsidiaries of the parent undertaking. The EU legislature also recognises that (i) transactions in derivatives which are objectively measurable as reducing risks directly relating to the commercial activity or treasury financing activity and (ii) intragroup transactions that serve group-wide liquidity or risk management purposes shall not be considered when determining the extent to which ancillary activities constitute a minority of activities at a group level for MiFID II purposes (see Article 2(4), fifth subparagraph, of MiFID II). To address this point, some respondents proposed that only entities that carry out banking activity as their *main* business should be	according to Regulation (EU) No 575/2013 of the European Parliament and of the Council[62], and any relevant assessments of relevant authorities in the Member State in which the institution concerned is established and other relevant materials. In line with normal supervisory practices, competent authorities will be able to challenge the assessment of institutions as to the comparability of third country regimes. **Groups of connected clients** The EBA clarifies that these guidelines only apply to exposures to individual counterparties, i.e. individual shadow banking entities, and do not require the creation of groups of connected clients. The large exposures regime, as set out in Regulation (EU) No 575/2013, applies independently of these guidelines.	

[62] The Commission's decision is available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.359.01.0155.01.ENG.

Summary of responses received	EBA analysis	Amendments to the proposals
captured by the guidelines. As an alternative, other respondents proposed that the *de minimis* exposure amount should be increased from 0.25% of a bank's capital to either 1% or €300m. **Consolidation:** Respondents supported the approach of excluding entities that are consolidated on an institution's balance sheet. It should be clarified that this applies also for entities consolidated on a voluntary basis, or entities that are subject to mandatory prudential consolidation under the CRR but are excluded from the scope of prudential consolidation on the basis of Article 19 of the CRR. **Equivalence of third country regimes:** In addition to scope issues, further clarity was sought on how the guidelines would work in practice in some areas. Most prominently, respondents noted a lack of clarity on how to judge whether a third country's prudential/regulatory requirements are 'equivalent' or 'comparable' to those applied under Union law. Respondents supported an approach that would allow institutions to make their own equivalence/comparability assessments – subject to ex post review of those assessments by the authorities. This is seen as advantageous, as it would avoid delays associated with centralised equivalence decisions. At a minimum, further details were requested on how equivalence decisions would be taken forward by authorities. The importance of this issue was seen as particularly high in the area of the requirements for credit institutions and insurers. In such cases, few equivalence decisions have yet been taken by the Commission– and thus exposures to banks or insurers in many third countries may unnecessarily fall into the scope of the		

Summary of responses received	EBA analysis	Amendments to the proposals
guidelines unless a practical solution is identified. One respondent queried whether an insurance company in a third country not considered to have an equivalent regime would be considered within the scope of the guidelines. **Groups of connected clients:** Finally, it remained unclear to some respondents how the guidelines would apply to groups of connected clients (GCCs). Further details were requested to explain (i) whether the guidelines would apply only to an entity within a GCC that met the relevant shadow banking definition, or whether the guidelines would instead capture the entire GCC as a single exposure, and (ii) the procedure to adopt in case of a classification of the parent company as an unregulated financial entity pursuant to Q&A 2013_492.		
Q2. Do you agree with the approach the EBA has proposed for the purposes of establishing effective processes and control mechanisms? If not, please explain why and present possible alternatives.		
{30 out of 57 respondents were silent on this question} According to a minority (4) of the respondents, this question should not be addressed at this stage, as establishing processes and control mechanisms is only possible once the scope of exposures under review has been clearly defined, or a full impact assessment has been conducted. Several of the respondents (8) broadly agree with the approach taken in allowing institutions to rely on their own internal framework and risk	The EBA notes the broad support for the guidelines' approach regarding the setting up of internal limits by the institutions. The EBA also notes the comments on the need to apply the guidelines in a proportional way. However, the EBA is of the view that risks posed by exposures to shadow banking entities need	No amendment.

Summary of responses received	EBA analysis	Amendments to the proposals
appetite to set internal limits. There is, however, also a substantial call (9) to introduce a principle of proportionality. This is justified because (i) the scope is so broad as to encompass entities which are very different in nature and not exposed to the same increased risks and (ii) the requirement to 'identify all potential risks [...] and the potential impact of those risks' is relatively broad and will result in operational challenges. According to their views, some exposures warrant very high levels of due diligence, whereas other exposures could easily be demonstrated to be less risky and less complex. The intensity and frequency of monitoring carried out should vary accordingly. Some respondents (4) stressed that it is important that the requirement for establishing effective process and effective mechanisms should be applied on a consolidated basis only, as: • Large exposure limits under CRR rules already apply at both solo and consolidated levels and so a sufficient backstop already exists within the current framework. • Applying the guidelines at consolidated level only would make it easier for institutions to manage the requirements within the ICAAP process, as individual legal entities may have only a partial view of the phenomenon. • The burden of infrastructure, systems and processes that institutions would need to put in place to comply with the guidelines would be kept proportionate.	to be monitored and managed regardless of the size, complexity or business model of the institution. The fact that institutions are allowed to set up internal limits as part of their risk assessment processes should ensure an application of the guidelines which is adequate to the institutions' risk profile. The EBA clarifies that these guidelines do not intend to introduce additional Pillar 2 requirements, but that the assessments should be done in the context of the regular Pillar 2 assessments, but with a focus on the shadow banking sector as a specific exposure class.	

Summary of responses received	EBA analysis	Amendments to the proposals
Some respondents (3) oppose aggregating limits, as they do not consider the targeted risk to be sectoral. It would be excessive to assume that shadow banking entities by their very nature have a default correlation close to one and thus pose a high concentration risk. Shadow banking entities are subject to (i) individual large exposure limits, (ii) a look-through approach to the ultimate underlying assets of a transaction and (iii) the limitation of exposures to individual counterparties or groups of connected clients under the current large exposure framework of the CRR. Some respondents therefore argued that an aggregate limit would give few additional benefits over the current framework. The targeted risk could be better addressed via ICAAP/Pillar 2, which specifically covers concentration risk, rather than the large exposure regime, which is intended to address default of single entities or groups of connected counterparties. It was requested that EBA clarify whether it wishes to introduce additional Pillar 2 requirements or whether compliance with the existing framework is sufficient, and whether the look-through requirements should be considered or not for the definition of the exposure. The assessment of the performed analyses could also be made consistent with the internal authorisation levels in the credit process. Some respondents (4) saw no issues of substance that would justify introducing additional specific Pillar II requirements relating to shadow bank exposures. In their opinion, requirements for institutions' risk management (credit risk, market risk, operational risk, etc.) are already sufficient to address shadow banking issues. Moreover, the use of Pillar 2 measures in such a		

Summary of responses received	EBA analysis	Amendments to the proposals
complex context might result in very heterogeneous implementation, thus endangering the level playing field among banks operating across borders. Furthermore the requirements regarding effective processes and control mechanisms, and oversight by the management body of the institutions as set out in the draft guidelines, would cause unnecessary additional administrative effort with few corresponding benefits.		
Q3. Do you agree with the approach the EBA has proposed for the purposes of establishing appropriate oversight arrangements?		
{37 out of 57 respondents were silent on this question} A significant number (8) of the respondents to this question share the EBA's view on the approach to oversight arrangements. This supports the view that institutions' management bodies must review and approve their shadow banking risk appetite and related risk management processes. Some respondents emphasised that attention should be paid to avoid duplication of work which would create additional burdens and overlaps. A minority of the respondents (3) explicitly opposed the idea of introducing separate qualitative requirements for exposures to shadow banks that are already part of Pillar II processes (e.g. internal risk management, governance of the institutions). These respondents do not see the need to add a specific layer for these broad bases of entities, as risk weighting criteria already exist for many of the transactions performed with clients/debtors or counterparties. One respondent even added that imposing such requirements is not covered by the mandate under Article 395(2) of the CRR.	The EBA notes the broad support for its proposals. The EBA agrees with the suggestion that the institution's management body could delegate certain reviews to senior management.	Amendment to the section on oversight by the management body of the institution.

Summary of responses received	EBA analysis	Amendments to the proposals
Another theme was that shadow banking entities should not be considered a single risk category. This could lead to underestimating risk for the risky exposures and over-allocation of risk management resources to the less risky exposures. Proportionality should be introduced taking into account the size, riskiness and nature of the exposures concerned. On a more practical side, it was also highlighted that the management body should be allowed to delegate necessary reviews to specialised and more relevant employees, such as the Chief Risk Officer and Risk Control function. Furthermore, sufficient time should be granted for the operationalisation of these requirements, e.g. via a phased implementation approach to avoid potential macrosystemic risks if banks are not in a position to use the principal approach on 1 January 2016. According to two respondents (2), it seems inappropriate to establish oversight arrangements before finalising a clear narrow definition of a shadow banking entity. Taking together a wide variety of vehicles may result in a very heterogeneous portfolio, the constituents of which are highly unlikely to impact an institution at the same time or in the same way. It seems unclear to these respondents how a bank would set a strategy and define a risk appetite for such a diverse group of exposures. Further, as the oversight arrangements cover such a wide array of exposures, it might distract the risk management's resources from the most risky ones. A full impact analysis is also requested, to show whether the sectoral definition applied for the aggregation under the shadow bank definition will result in a population which behaves in a correlated fashion.		
Q4. Do you agree with the approaches the EBA has proposed for the purposes of establishing aggregate and individual limits?		

Summary of responses received	EBA analysis	Amendments to the proposals
{31 out of 57 respondents were silent on this question} Some respondents (5) agreed in principle with the proposed approach and welcomed the principle of proportionality reflected within it. Opponents (7) claimed that no risk management benefits would be generated by the guidelines, as banks' routine lending processes and strategies for managing credit risk are already sufficiently robust. The approach was also criticised for potentially working against the objectives of Capital Market Union. Whereas a few (2) suggest having a limit at the aggregate level, most of the respondents (8) have significant reservations regarding the requirement for institutions to set an aggregate limit to the entire shadow banking sector. These concerns were particularly based on the heterogeneity of the targeted population, which would make calibration of an objectively 'appropriate' aggregate limit difficult. Individual limits were preferred by these respondents, as they could be calibrated more simply, and would better fit with the philosophy of the large exposure regime[63]. Those concerned with the calibration of aggregate limits requested that an impact study be undertaken. Further, they advocated the introduction of the following amendments: • Reduction of the scope of the guideline so as exclude all UCITS,	The EBA recognises the role the shadow banking sector plays in providing alternative sources of funding to the real economy. Given this, the EBA considers it premature to use the guidelines to introduce a quantitative limit to institutions' individual or aggregated exposures to these shadow banking entities. The approach described in the guidelines allows institutions to set risk tolerance levels for exposures to shadow banking entities, corresponding to their risk appetite, within their overall business model and risk management framework, with competent authorities retaining the ability to take supervisory measures where appropriate. This approach places the responsibility on institutions to demonstrate that the risks related to exposures to shadow banking entities are being managed effectively, in particular by improving, where necessary, the due diligence carried out concerning these exposures.	No amendment.

[63] The large exposure regime is traditionally designed to act as a backstop to individual client limits rather than to address sectoral credit concentration risk.

Summary of responses received	EBA analysis	Amendments to the proposals
and AIFs without substantial leverage, including VNAV MMFs. • Preferential treatment of exposures related to central clearing activities. • Exemption for certain custody-related services. • Increase of the materiality threshold. Should the EBA decide to introduce new limits, some respondents advocated either a blanket aggregate limit[64] or a general individual limit to shadow banking entities of 20% of eligible capital subject to the condition that the definition of shadow banking entities is narrowed. If these alternatives are not considered acceptable and the idea of establishing both individual and aggregate limits is retained, it was considered essential to drop the fallback approach. The issue was also raised whether the draft guidelines go significantly beyond the CRR mandate in setting out a combination of aggregate and individual limits.		
Q5. Do you agree with the fallback approach the EBA has proposed, including the cases in which it should apply? If not, please explain why and present possible alternatives. **Do you think that Option 2 is preferable to Option 1 for the fallback approach? If so, why? In particular:**		

[64] For example, at a level of between 500% and 800% of eligible capital.

Summary of responses received	EBA analysis	Amendments to the proposals
Do you believe that Option 2 provides more incentives to gather information about exposures than Option 1? **Do you believe that Option 2 can be more conservative than Option 1? If so, when?** **Do you see some practical issues in implementing one option rather than the other?**		
{34 out of 57 respondents were silent on this question} A few respondents found it hard to agree or disagree with the fallback approach, as there is no justification as to why the 25% limit would be relevant. Some respondents expressed concern that the proposed fallback approach is unlikely to serve as an effective risk management tool, as it is quite blunt and might ignore the materiality aspect, which is part of every loan decision. Further, the need for a fallback was questioned, given that shortcomings in setting internal credit exposure limits can be addressed under the SREP. In addition, concerns were raised that this approach may run the risk of setting a de facto limit of 25% should banks be unable to meet the data requirements that would enable them to use the principal approach by 1 January 2016. If a fallback approach will be applied, the majority tended to favour Option 2. The following reasons were cited: • Shadow banking entities will be a very heterogeneous group with different business models, levels of disclosure and risk levels within their portfolios. Based on this heterogeneity, it does not seem appropriate that, if a credit institution gathers all required information for the majority of those entities but, for a small group of entities, cannot obtain the information required to set a	The EBA has given great consideration to the feedback received in the context of the consultation and has changed the design of the fallback option. The rationale was threefold. First of all, one the objectives of the guidelines is to create appropriate incentives for institutions to have in place the right processes and procedures to gather information on shadow banking entities. In this sense, the incapacity of an institution to get information on a minor part (or even on one only) of its exposures to shadow banking entities would de facto hinder the incentives for the 'search for information' also with reference to the other exposures to shadow banking entities. The EBA has also considered the importance of the coherence between the fallback approach and the concept of the 'unknown client' defined in the delegated regulation regarding the treatment of	The fallback approach has been redefined along the lines of Option 2 in the consultation paper.

Summary of responses received	EBA analysis	Amendments to the proposals
meaningful limits framework, all the bank's exposures to all shadow banking entities - regardless of the information obtained - should be perceived as an exposure to the 'same client' and, as such, will be subject to a 25% aggregate limit. • Option 2 makes better use of available information and provides stronger incentives to gather information about shadow banking exposures by rewarding the collection and use of pertinent data with appropriate and realistic exposure limits. • Option 2 is better aligned with the rationale of the large exposure framework to prevent institutions from incurring disproportionately large losses as a result of the failure of an individual client or group of connected clients due to the occurrence of unforeseen events. • Option 2 is better aligned with the approach of the RTS regarding the treatment of transactions with underlying assets. Here, the 'unknown client' bucket is only required for those exposures for which an institution fails to meet the specific principal requirements of the RTS. • The Option 2 approach is not unknown outside the area of large exposures, as it applies, for example, to investments in financial sector entities for purposes of capital deductions. • Option 2 leads to less overestimation of the total population in	exposures to transactions with underlying assets. Finally, the EBA is aware that a fallback approach based on Option 1 of the consultation paper might not fully respect the proportionality principle, which is one of the crucial elements of EU prudential regulation. Given the above, therefore, the EBA decided that the fallback approach should be implemented in a way that is coherent with Option 2 of the consultation paper. In particular, the fallback approach will be applied: i) to all exposures to shadow banking entities if institutions cannot meet the requirements regarding effective processes and control mechanisms or oversight by their management board; and ii) if institutions meet the above requirements of processes, control and oversight, only to those exposures to shadow banking entities for which sufficient information is unavailable. Regarding the calibration, results of the data collection show that a limit of 25% of the institution's eligible capital on aggregate exposures to shadow banking entities would have an impact on around half of the credit institutions and investment firms which reported individual exposures equal or above 0.25% of its eligible capital (i.e. 65 institutions	

Summary of responses received	EBA analysis	Amendments to the proposals
case of difficulty eliminating exempt institutions from their datasets. Option 1 is perceived by some as unnecessarily punitive and not in line with the development of enhanced risk-sensitive regulatory frameworks and internal modelling. In addition it does not provide incentives to develop a robust assessment process, as non-compliance with the principal approach for just one shadow banking exposure will lead to an overall limit to all shadow banking exposures. Furthermore, Option 1 could lead, in the short term, to swift systemic events resulting from the insolvency/fire sale of assets from the shadow banking entities that cannot provide the necessary information to the banking sector. The limit may need to be considerably higher than 25%, as banks may lend up to 25% of their eligible capital to each shadow banking entity with which they do business. A Quantitative Impact Study is requested before such an aggregate limit is set. Additionally, if the guidelines were to come into force without a suitable grandfathering arrangement, the institutions would be forced to terminate some of their current exposures before the agreed terms, with unforeseeable consequences for the markets.	of the total of 184 institutions that participated in the data collection). However, it should be noted that the results of the data collection are very conservative given that a much wider definition of 'shadow banking entity' was used for purposes of the data collection than the definition used in these guidelines and that the simulations assume that all exposures would be captured by the fallback approach (Option 1 in the consultation paper). It is also noted that the number of individual exposures which are above 25% of the institution's eligible capital is extremely negligible (around 0.01% of all exposures reported). Everything considered and taking into account the risky nature of these exposures, the EBA believes it would be prudentially sound to align the fallback approach with the large exposures limits of 25% of eligible capital (with possible exceptions for positions in the trading book which meet the conditions in Article 395(5) of the CRR and could therefore exceed the 25% limit) to provide a backstop to exposures to counterparties for which the institution is not able to collect sufficient information to set out an internal limit.	
Q6. Taking into account, in particular, the fact that the 25% limit is consistent with the current limit in the large exposures framework, do you agree it is an adequate limit for the fallback approach? If not, why?		

Summary of responses received	EBA analysis	Amendments to the proposals
What would the impact of such a limit be in the case of Option 1? And in the case of Option 2?		
{34 out of the 57 respondents were silent on this question} Only a few respondents explicitly agree that the 25% limit is an appropriate limit for the fallback approach. The inclusion of a 'fallback' approach could run the risk of setting a de facto aggregate limit of 25%, as it is unlikely banks will be able to meet the data requirements to allow use of the principal approach from 1 January 2016. This in itself could pose a macrosystemic risk if most or all banks are forced to use the fallback approach from day one. For example, this may spark fire sales, thereby destabilising markets, leading to withdrawal of finance and affecting credit mediation. The majority of the respondents state that the 25% aggregate limit proposed under the fallback approach is overly conservative and onerous and lacks a robust justification. The assumption of interconnectedness is deemed erroneous and unrealistic. The mere fact that banks gather insufficient information to allow compliance with the specific rules of the principal approach does not imply that all the shadow banking exposures are highly correlated or should be connected. The variety of entities grouped together does not pose a single risk to an institution and should not be understood as the same client. The EBA should refrain from introducing elements related to geographic and sectoral risks that conflict with the existing policy framework for large exposures and the forthcoming framework of the BCBS. A limit of 25% applied sectorally is likely to lead to a need for exposure reductions by institutions, thereby	These guidelines will apply from 01.01.2017, therefore allowing sufficient time for institutions to prepare to meet the data requirements that are required to use the principal approach. The EBA notes the concerns regarding the 25% aggregate limit (fallback approach) and draws attention to its response to Q5. The EBA agrees with the consultation feedback pertaining to geographic and sectoral risks and therefore considers it unnecessary to assess exposures via this categorisation. The EBA has considered the proposed alternative to segment shadow banking exposures and has rejected it, as it is deemed too onerous to implement in practice and would not ultimately ensure a harmonised application of the guidelines and a level playing field and would not allow meaningful comparisons, as each institution may define different segments.	No amendment.

Summary of responses received	EBA analysis	Amendments to the proposals
having a potential impact on the supply of credit to SMEs and hampering growth as well as restraining recent efforts to revive the securitisation market. As an alternative, some respondents suggest that banks might have the possibility to segment shadow banking exposures between specific sub-groups. Where it is possible to prove that no correlation is observed within a sub-group, individual limits for shadow banking entities should be sufficient - even if the remaining data requirements are not totally fulfilled. In addition to the main distinction based on the prudential framework, some consider that the criteria of the nature of the activity, the level of risk and the possibility of 'run' effects could be used to introduce granularity in the treatment of shadow banking entities. If a fallback approach is nevertheless retained, then an appropriate limit, much higher than 25%, would need to be considered. Using the same percentage for an aggregate limit to the whole shadow banking sector as the one currently used for the large exposure limit of Article 395 of the CRR indicates that the proposed percentage is much too low. Reference was made to the aggregate limit for all large exposures (exposures exceeding the 10% threshold) of 800% of own funds in Directive 2006/48/EC (CRD II), a limit in the three-digit range or a whole-number multiplier of an institution's capital base.		