COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Luxembourg, le 19 mars 2013

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

CIRCULAIRE CSSF 13/563

Concerne: Mise à jour de la circulaire CSSF 12/552 relative à l'administration centrale, la gouvernance interne et la gestion des risques

Mesdames, Messieurs,

La présente circulaire modifie la circulaire CSSF 12/552 en y incorporant les orientations de l'Autorité bancaire européenne (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'Autorité européenne des marchés financiers (ESMA) concernant certains aspects de la directive 2004/39/CE (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 de l'ESMA concernant certains aspects de la directive MIF relatifs aux exigences à l'encontre de la fonction compliance exposent des considérations relatives au rôle et aux responsabilités de la fonction compliance découlant de la directive MIF. Ces orientations se déclinent en « orientations générales » et « orientations complémentaires » qui donnent des précisions supplémentaires sur les orientations générales. Les orientations générales de l'ESMA se confondent largement avec les règles générales sur la fonction compliance énoncées au chapitre 6 de la circulaire CSSF 12/552 et ne constituent donc pas une nouveauté à part entière pour les établissements de crédit et entreprises d'investissement. Lorsqu'ils mettent en œuvre la fonction compliance relative à la fourniture de services d'investissement suivant la directive MIF, les établissements doivent tenir compte des « orientations complémentaires » formulées dans le document ESMA/2012/388.

Les orientations de l'EBA en matière d'éligibilité des administrateurs, directeurs autorisés et responsables de fonctions clés apportent des précisions, au niveau du chapitre 4 de la circulaire CSSF 12/552 et notamment des sections 4.1.1., 4.1.2. et

[*] 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 reste applicable. La présente circulaire ne change en rien les obligations qui incombent à ces professionnels.

4.2.2., en ce qui concerne les principes directeurs à arrêter par le conseil d'administration en matière de sélection, d'évaluation, de mesures correctrices et de documentation des nominations aux postes clé, y compris les mandats d'administrateur et de directeur autorisé d'un établissement de crédit ou d'une entreprise d'investissement. Il revient à chaque établissement de crédit et entreprise d'investissement de dresser par écrit la liste de ces fonctions clé, compte tenu du principe de proportionnalité. Toutefois, la CSSF considère que la définition des fonctions clé couvre au minimum les administrateurs, les directeurs autorisés et les responsables des 3 fonctions de contrôle interne.

1. La circulaire CSSF 12/552 est modifiée conformément à l'annexe.

   L'annexe en question présente les changements apportés par la présente à la circulaire CSSF 12/552 en version « suivi des modifications » afin de faciliter la lecture et la compréhension.

2. Les modifications apportées par la présente circulaire à la circulaire CSSF 12/552 entrent en vigueur conformément aux dispositions du point 241 de la partie IV de la circulaire CSSF 12/552. Il s'ensuit que les nouvelles exigences découlant de l'orientation ESMA/2012/388 s'appliqueront à partir du 1er juillet 2013. Les nouvelles exigences résultant de l'orientation EBA/GL/2012/06 s'appliqueront à partir du 1er juillet 2013, exception faite pour l'évaluation des compétences professionnelles et qualités personnelles des membres du conseil d'administration qui sera soumise aux dispositions de la circulaire CSSF 12/552 à partir du 1er janvier 2014.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Simone DELCOURT	Jean GUILL
Directeur	Directeur	Directeur général

Annexe

Annexe

Luxembourg, le 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 la circulaire CSSF 13/563

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

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 d'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 »). 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.

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

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.

[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.

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 ;

   ~~5)~~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.

   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.

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

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 ~~à des~~ aux fonctions clé de l'établissement, ~~y compris aux postes d'administrateur et de directeur autorisé et comprenant les critères d'éligibilité pour accéder à ces fonctions,~~ ainsi que les procédures régissant le conseil d'administration en termes de sa composition, de ses responsabilités, de son organisation et de son fonctionnement.[4] Les principes directeurs régissant la nomination et la succession aux fonctions clé de l'établissement stipulent qu'en la matière, ~~e~~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 assessment of the suitability of members of the management body and key function holders* - EBA/GL/2012/06).

[4] 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.

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[5] - 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.

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.

[5] Y inclus une relation salariale

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[6]

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 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[7]:

    - le suivi du processus d'élaboration de l'information financière,

[6] 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.

[7] 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.

- 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.

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[8] 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 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

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

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 ~~la fonction~~ le poste de « Chief Compliance Officer » suivant le point 141, ne peut pas en même temps être responsable pour 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 ~~fonctions~~ 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.[9]

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.

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,

[9] 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.

- 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 ~~les meilleurs délais en communiquant~~le respect de la procédure prudentielle d'approbation des titulaires de fonctions clé telle que publiée par ~~ailleurs les motifs expliquant la révocation.~~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 ~~importantes~~ :
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 ~~importantes~~ :
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 ~~les~~ en évalue ~~pour en déterminer~~ l'importance ~~ainsi que~~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 ~~importante~~ :
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 reconnus10,
- 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

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

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,
- 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.[11]

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

[11] 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. ».

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;
- 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;
- 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 221 et 222.

    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.

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

241. 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;
- 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.

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

243. 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.

244. 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).

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON
Directeur

Simone DELCOURT
Directeur

Jean GUILL
Directeur général