cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 20/758

Administration centrale, gouvernance interne et gestion des risques

Commission de Surveillance du Secteur Financier

Circulaire CSSF 20/758

Concerne : Administration centrale, gouvernance interne et gestion des risques

Luxembourg, le 7 décembre 2020

À toutes les entreprises d'investissement

Mesdames, Messieurs,

Les articles 17 paragraphe 1bis et 38-1 de la loi du 5 avril 1993 relative au secteur financier (« LSF »), complétés par le règlement CSSF N° 15-02 relatif au processus de contrôle et d'évaluation prudentiels (« RCSSF 15-02 »)[1] exigent des entreprises d'investissement qu'elles 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 elles sont ou pourraient être exposées, 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.

La présente circulaire précise les mesures que doivent prendre les entreprises d'investissement en exécution des dispositions de la LSF et du RCSSF 15-02[2] en matière d'administration centrale, de gouvernance interne et de gestion des risques. Elle reprend les principes, orientations et recommandations européennes et internationales qui s'appliquent en la matière, en les inscrivant de manière proportionnée dans le contexte du secteur financier luxembourgeois. Lorsqu'en raison de la taille, de la nature et de la complexité des activités et de l'organisation, l'application du principe de proportionnalité demande une administration centrale, une gouvernance interne ou une gestion des risques renforcées, les établissements se reportent aux principes énoncés à la partie I, chapitre 2 ainsi qu'aux orientations et recommandations précitées pour guider cette mise en œuvre. Ceci vaut en particulier pour les orientations de l'Autorité bancaire européenne (« EBA ») en matière de gouvernance interne (Guidelines on internal governance « EBA/GL/2017/11 ») et les orientations communes de l'EBA et de l'Autorité européenne des marchés financiers (« ESMA ») en matière d'éligibilité des membres d'organe de direction et des titulaires de fonctions clés (Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders « EBA/GL/2017/12 »).

[1] *Le RCSSF 15-02 s'applique uniquement aux établissements CRR, c'est-à-dire, aux établissements de crédit et aux entreprises d'investissement CRR.*

[2] *Idem*

Commission de Surveillance du Secteur Financier

La présente circulaire abroge et remplace la circulaire CSSF 12/552 sur l'administration centrale, la gouvernance interne et la gestion des risques (telle que modifiée par les circulaires CSSF 13/563, 14/597, 16/642, 16/647, 17/655 et 20/750), dans le chef des entreprises d'investissement.

S'agissant de nominations d'administrateurs, de directeurs autorisés et de titulaires de fonctions clés, la présente circulaire doit se lire en parallèle avec la Procédure prudentielle en la matière publiée sur le site internet de la CSSF.

La circulaire est divisée en quatre parties : la première partie contient les définitions et le champ d'application ; la deuxième partie, les exigences de structure en matière d'administration centrale et de gouvernance interne ; la troisième partie, les exigences spécifiques en matière de gestion des risques et la quatrième partie, l'entrée en vigueur de la présente circulaire.

Commission de Surveillance du Secteur Financier

TABLE DES MATIÈRES / TABLE OF CONTENTS

Partie I. Définitions et champ d'application 7
Chapitre 1. Définitions et abréviations 7
Chapitre 2. Champ d'application et proportionnalité 8
Partie II. Dispositif en matière d'administration centrale et de gouvernance interne 11
Chapitre 1. L'administration centrale 11
Chapitre 2. Le dispositif de gouvernance interne 11
Chapitre 3. Propriétés génériques d'un dispositif « solide » en matière d'administration centrale et de gouvernance interne 13
Chapitre 4. Conseil d'administration et direction autorisée 14
Sous-chapitre 4.1. Le conseil d'administration 14
Section 4.1.1. Responsabilités du conseil d'administration 14
Section 4.1.2. Composition et qualification du conseil d'administration 18
Section 4.1.3. Organisation et fonctionnement du conseil d'administration 20
Section 4.1.4. Comités spécialisés 21
Sous-section 4.1.4.1. Le comité d'audit 22
Sous-section 4.1.4.2. Le comité des risques 24
Sous-chapitre 4.2. La direction autorisée 25
Section 4.2.1. Responsabilités de la direction autorisée 25
Section 4.2.2. Qualification de la direction autorisée 29
Chapitre 5. Organisation administrative, comptable et informatique 29
Sous-chapitre 5.1. L'organigramme et les ressources humaines 29
Sous-chapitre 5.2. Les procédures et la documentation interne 31
Sous-chapitre 5.3. L'infrastructure administrative et technique 32
Section 5.3.1. L'infrastructure administrative des fonctions commerciales 32
Section 5.3.2. La fonction financière et comptable 32
Section 5.3.3. La fonction informatique 34
Section 5.3.4. Le dispositif de communication et d'alerte interne et externe 34
Section 5.3.5. Le dispositif de gestion de crises 35
Chapitre 6. Le contrôle interne 36
Sous-chapitre 6.1. Les contrôles opérationnels 37
Section 6.1.1. Contrôles quotidiens réalisés par le personnel exécutant 37
Section 6.1.2. Contrôles critiques continus 37

Section 6.1.3. Contrôles réalisés par les membres de la direction autorisée sur les activités ou fonctions qui tombent sous leur responsabilité directe 38
Sous-chapitre 6.2. Les fonctions de contrôle interne 38
Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne 39
Section 6.2.2. Caractéristiques des fonctions de contrôle interne 39
Section 6.2.3. Exécution des travaux des fonctions de contrôle interne 41
Section 6.2.4. Organisation des fonctions de contrôle interne 42
Section 6.2.5. La fonction de contrôle des risques 46
Sous-section 6.2.5.1. Champ d'application et responsabilités spécifiques de la fonction de contrôle des risques 46
Sous-section 6.2.5.2. Organisation de la fonction de contrôle des risques 47
Section 6.2.6. La fonction compliance 48
Sous-section 6.2.6.1. La charte de compliance 48
Sous-section 6.2.6.2. Champ d'application et responsabilités spécifiques de la fonction compliance 49
Sous-section 6.2.6.3. Organisation de la fonction compliance 52
Section 6.2.7. La fonction d'audit interne 52
Sous-section 6.2.7.1. La charte d'audit interne 52
Sous-section 6.2.7.2. Responsabilités spécifiques et champ d'application de la fonction d'audit interne 54
Sous-section 6.2.7.3. Exécution des travaux d'audit interne 55
Sous-section 6.2.7.4. Organisation de la fonction d'audit interne 57
Chapitre 7. Exigences spécifiques 57
Sous-chapitre 7.1. Structure organisationnelle et entités juridiques (« Know-your-structure ») 57
Section 7.1.1. Structures complexes et activités inhabituelles ou potentiellement non transparentes 58
Sous-chapitre 7.2. Gestion des conflits d'intérêts 58
Section 7.2.1. Exigences spécifiques relatives aux conflits d'intérêts en relation avec des parties liées 60
Sous-chapitre 7.3. Procédure d'approbation des nouveaux produits (« New Product Approval Process ») 60
Sous-chapitre 7.4. Sous-traitance (« Outsourcing ») 61
Section 7.4.1. Exigences générales en matière de sous-traitance 62

Section 7.4.2. Exigences particulières en matière de sous-traitance dans le domaine informatique 65
Sous-section 7.4.2.1. Services de gestion/d'opération des systèmes informatiques 65
Sous-section 7.4.2.2. Services de conseil, de développement et de maintenance 66
Sous-section 7.4.2.3. Services d'hébergement et propriété de l'infrastructure 66
Section 7.4.3. Exigences générales supplémentaires 67
Section 7.4.4. Documentation 68
Chapitre 8. Reporting légal 69
Partie III. Gestion des risques 69
Chapitre 1. Principes généraux en matière de mesure et de gestion des risques 69
Sous-chapitre 1.1. Le cadre de gestion des risques à l'échelle de l'établissement 69
Section 1.1.1. Généralités 69
Section 1.1.2. Politiques spécifiques (de risque, de fonds propres et de liquidités) 69
Section 1.1.3. Détection, gestion, mesure et déclaration des risques 71
Chapitre 2. Risques de concentration 72
Chapitre 3. Tarification du risque (« Risk Transfer Pricing ») 72
Chapitre 4. Gestion de fortune et activités associées (activités de « private banking ») 73
Chapitre 5. Risques liés aux entités shadow banking 74
Sous-chapitre 5.1. Mise en œuvre de principes de contrôle interne solides 74
Sous-chapitre 5.2. Application de limites quantitatives 75
Chapitre 6. Risque de taux d'intérêt 77
Sous-chapitre 6.1. Risque de taux d'intérêt inhérent aux activités autres que de négociation 77
Sous-chapitre 6.2. Corrections de la duration modifiée des titres de créance 77
Chapitre 7. Risques liés à la conservation d'actifs financiers par des tiers 78
Partie IV. Entrée en vigueur 78

Partie I. Définitions et champ d'application

Chapitre 1. Définitions et abréviations

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. La réglementation du secteur financier alloue aux conseils d'administration des entreprises d'investissement des responsabilités en matière de surveillance et de contrôle, ainsi qu'en matière de détermination et d'approbation des orientations stratégiques et politiques clés. Le terme de « conseil d'administration » n'est pas à prendre dans son acceptation juridique, puisque les 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 dans une organisation dualiste, ce dernier assumera les responsabilités que la présente circulaire attribue au « conseil d'administration ». Le conseil d'administration correspond également à l'organe de direction dans sa fonction de surveillance selon les EBA/GL/2017/11.
   2) « direction autorisée » ou « directeurs autorisés » : les personnes visées à l'article 19 paragraphe 2 de la LSF. D'un point de vue prudentiel, la direction autorisée est responsable de la gestion journalière d'une entreprise d'investissement, conformément aux orientations stratégiques et politiques clés approuvées par le conseil d'administration. La direction autorisée est également assimilée à l'organe de direction dans sa fonction exécutive selon les EBA/GL/2017/11.

      Dans un système moniste, les directeurs autorisés peuvent être membres du conseil d'administration, alors que dans un système dualiste, la direction autorisée correspond au directoire.

   3) « entreprise d'investissement CRR » : une entreprise d'investissement au sens de l'article 4, paragraphe 1er, point 2) du règlement (UE) n° 575/2013.
   4) « entreprise d'investissement non CRR » : une entreprise d'investissement autre qu'une entreprise d'investissement CRR.
   5) « « établissement(s) » ou « entreprise(s) d'investissement » » : les entreprises d'investissement CRR et les entreprises d'investissement non CRR de droit luxembourgeois, y compris leurs succursales, les succursales luxembourgeoises d'entreprises d'investissement de pays tiers ainsi que les succursales luxembourgeoises d'entreprises d'investissement agréées dans un autre Etat membre.

6) « établissement d'importance significative » : pour les besoins de la présente circulaire, une entreprise d'investissement d'importance systémique suivant l'article 59-3 de la LSF et, le cas échéant, les autres entreprises d'investissement déterminées par la CSSF sur base de l'évaluation de la taille et de l'organisation interne des entreprises d'investissement ainsi que de la nature, de l'échelle et de la complexité de leurs activités.
7) « ICAAP » : Internal Capital Adequacy Assessment Process.
8) « ILAAP » : Internal Liquidity Adequacy Assessment Process.
9) « LSF » : la loi modifiée du 5 avril 1993 relative au secteur financier.
10) « MiFID » : Markets in Financial Instruments Directive.
11) « organe de direction » : l'organe de direction, suivant la définition de la LSF, correspond à l'organe de direction dans sa fonction de surveillance et dans sa fonction exécutive selon les EBA/GL/2017/11. Il désigne le conseil d'administration et la direction autorisée d'un établissement pourvu d'une organisation moniste ou le conseil de surveillance et le directoire d'un établissement pourvu d'une organisation dualiste.
12) « parties liées » : les entités (structures) juridiques appartenant au groupe auquel l'établissement appartient ainsi que les membres du personnel, actionnaires, directeurs et membres du conseil d'administration de ces entités.
13) « Procédure prudentielle » : procédure prudentielle d'approbation des administrateurs, directeurs autorisés et titulaires de fonctions clés auprès des entreprises d'investissement.
14) « règlement CRR » : le règlement (UE) n° 575/2013 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement.
15) « titulaires de fonctions clés » : les responsables des fonctions dont l'exercice permet d'avoir une influence notable sur la conduite ou le contrôle des activités des établissements. Ils comprennent en particulier les responsables des trois fonctions de contrôle interne auprès de l'ensemble des établissements, à savoir : le Chief Risk Officer (« CRO ») pour la fonction de contrôle des risques, le Chief Compliance Officer (« CCO ») pour la fonction compliance et le Chief Internal Auditor (« CIA ») pour la fonction d'audit interne, ainsi que le responsable de la fonction financière (Chief Financial Officer, « CFO ») auprès des établissements d'importance significative.

Chapitre 2. Champ d'application et proportionnalité

2. La circulaire s'applique aux entreprises d'investissement de droit luxembourgeois, y compris leurs succursales, ainsi qu'aux succursales luxembourgeoises d'entreprises d'investissement de pays tiers.

Pour les domaines où la CSSF conserve une responsabilité de contrôle en tant qu'autorité d'accueil - il s'agit notamment des mesures en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi que des règles applicables en matière de fourniture de services d'investissement - les succursales luxembourgeoises d'entreprises d'investissement agréées dans un autre Etat membre mettent en place en coordination avec cette entreprise agréée 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.

3. La circulaire s'applique aux établissements sur une base individuelle, sous-consolidée et consolidée ainsi qu'aux compagnies financières holding ou aux compagnies financières holding mixtes visées à l'article 49(2) points a) à c) de la LSF.

   Si l'établissement est une entreprise mère (tête de groupe), la circulaire s'applique alors au « groupe » dans son ensemble : à l'entreprise mère ainsi qu'aux différentes entités juridiques qui composent ce groupe – qu'elles soient incluses ou non dans le périmètre de consolidation prudentielle suivant le règlement CRR - y compris les succursales, dans le respect des lois et des dispositions réglementaires nationales qui s'appliquent aux entités en question.

   Ainsi, quelle que soit la structure organisationnelle et opérationnelle de l'établissement ou d'un groupe, 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, y compris les activités et les risques intragroupe et peu importe la localisation des risques.

   Les mesures d'exécution que les établissements prennent en vertu de la présente circulaire sont proportionnelles à leur taille et à leur organisation interne ainsi qu'à la nature, à l'échelle et à la complexité de leurs activités, y compris les risques. 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, de gouvernance interne et de gestion des risques. Ce dispositif renforcé comprend par exemple, l'instauration de comités spécialisés, la nomination de membres indépendants additionnels au conseil d'administration ou encore de directeurs autorisés supplémentaires pour faciliter la gestion journalière.

A l'opposé, pour des établissements dont la taille, l'organisation interne ainsi que la nature, l'échelle et la complexité des activités sont moindres, le principe de proportionnalité peut jouer à la baisse. Ainsi, un établissement ayant des activités limitées et peu complexes peut fonctionner adéquatement au sens de la présente circulaire en désignant des responsables des fonctions compliance et de contrôle des risques à temps partiel (sans remettre en cause le principe de permanence de la fonction) ou en sous-traitant l'exécution des tâches opérationnelles de l'audit interne entièrement ou partiellement. 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.

Au niveau de la direction autorisée, alors que la répartition des tâches s'effectue dans le respect du principe de la ségrégation des tâches, la responsabilité reste collective.

La mise en œuvre du principe de proportionnalité tient compte des éléments suivants :

a. la forme juridique et la structure de propriété et de financement de l'établissement ;
b. le modèle d'affaires et la stratégie en matière de risque ;
c. la taille de l'établissement et de ses filiales ainsi que la nature et la complexité des activités (y compris le type de clientèle et la complexité des produits ou contrats) ;
d. la nature et la complexité de la structure organisationnelle et opérationnelle, y compris l'empreinte géographique, les canaux de distribution et les activités sous-traitées ;
e. la nature et l'état des systèmes d'information et dispositifs de continuité.

Quelle que soit l'organisation retenue, les arrangements en la matière permettent à l'établissement d'opérer dans le plein respect des dispositions prévues à la partie II de la présente circulaire. Les établissements documentent par écrit leur analyse en matière de proportionnalité et en font approuver les conclusions par le conseil d'administration.

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

Chapitre 1. L'administration centrale

1. 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.

2. Le centre de prise de décision comprend la direction autorisée ainsi que les responsables des fonctions commerciales, des fonctions de support et de contrôle et des différentes unités opérationnelles existant à l'intérieur de l'établissement.

3. Le centre administratif comprend l'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 délai.

4. Lorsque l'établissement est tête de groupe, 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 légal.

Chapitre 2. Le dispositif de gouvernance interne

5. La gouvernance interne est une composante 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.

6. La gouvernance interne doit assurer la gestion saine et prudente des activités, y compris des risques qui leur sont inhérents. 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 ;
- des mécanismes adéquats de contrôle interne qui répondent aux dispositions du chapitre 6 de cette partie. 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, 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 ;
- un processus clair de prise de risques comprenant un appétit au risque formellement et précisément arrêté dans tous les domaines d'activité, un processus décisionnel rigoureux, des analyses de qualité et des limites ;
- des processus de détection, de mesure, de déclaration, de gestion, d'atténuation et de contrôle des risques auxquels les établissements sont ou pourraient être exposés ;
- 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 ;
- une procédure formelle d'escalade, de règlement et de sanction des problèmes, déficiences et irrégularités relevés par le biais des mécanismes de contrôle et d'alerte internes ;
- 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 clés 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 ;
- un dispositif de gestion de crises qui assure une capacité de réaction appropriée en cas de crise, y compris un plan de redressement conforme aux exigences du chapitre 2 de la partie IV de la LSF.

7. Tout établissement promeut une culture interne du risque et de la conformité 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.

Cette culture généralisée des risques et de la conformité, forte et omniprésente, doit également se refléter dans les stratégies, politiques et procédures de l'établissement, les formations proposées et les messages véhiculés aux membres du personnel en ce qui concerne la prise et la gestion des risques au sein de l'établissement. Une telle culture se caractérise par l'exemple donné par le conseil d'administration et la direction autorisée (« tone from the top ») et implique la responsabilisation de tous les membres du personnel pour leurs actes et comportements, un dialogue ouvert et critique et l'absence d'incitation à une prise de risque inappropriée.

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

8. 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, tout établissement se dote 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 par rapport 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 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 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 ;

- soit conforme aux exigences légales et réglementaires, y compris par rapport aux exigences de la présente circulaire (« conformité »).

9. 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.

10. Les entreprises d'investissement CRR publient les éléments clés en matière de gouvernance interne et de gestion des risques conformément aux dispositions du règlement CRR (article 435 et titre Ier de la huitième partie) ainsi qu'aux orientations relatives aux exigences de publication de l'EBA (Guidelines on disclosure requirements under Part Eight of Regulation (EU) No 575/2013, « EBA/GL/2016/11 »).

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

11. Le conseil d'administration a la responsabilité globale de l'établissement. Il définit, surveille et porte la responsabilité de la mise en place d'un solide dispositif en matière d'administration centrale, de gouvernance et de contrôle interne, qui comprend une organisation interne clairement structurée et des fonctions de contrôle interne indépendantes ayant une autorité, une importance et des ressources appropriées à leurs responsabilités. Le cadre mis en place doit permettre d'assurer la gestion saine et prudente de l'établissement, d'en préserver la continuité et d'en protéger la réputation. A cette fin, le conseil d'administration approuve et arrête par écrit, après avoir entendu la direction autorisée et les responsables des fonctions de contrôle interne, les éléments clés suivants du dispositif en matière d'administration centrale, de gouvernance interne et de gestion des risques :
    - la stratégie commerciale (modèle d'affaires) de l'établissement dans le respect des intérêts financiers de l'établissement à long terme, de sa solvabilité, de sa situation des liquidités et de son appétit au risque. Le développement et le maintien d'un modèle d'affaires durable exige la prise en compte de tous les risques matériels, y compris les risques environnementaux, sociaux et de gouvernance ;
    - la stratégie de l'établissement en matière de risques, y compris l'appétit au risque et le cadre global de prise et de gestion des risques de l'établissement ;

- la stratégie de l'établissement en matière de fonds propres et de réserves de liquidités réglementaires et internes ;
- une structure organisationnelle et opérationnelle claire et cohérente qui règle en particulier la création et le maintien par l'établissement d'entités (structures) juridiques ;
- les principes directeurs en matière de systèmes, de technologie et de sécurité de l'information conformément à la circulaire CSSF 20/750, y compris les dispositifs internes de communication et d'alerte ;
- les principes directeurs relatifs aux mécanismes de contrôle interne, qui incluent les fonctions de contrôle interne ;
- les principes directeurs en matière de politique de rémunération ;
- les principes directeurs en matière de déontologie, de valeurs d'entreprise et de gestion des conflits d'intérêts ;
- les principes directeurs en matière d'escalade et de sanctions visant à assurer que tout comportement non respectueux des règles applicables soit adéquatement poursuivi et sanctionné ;
- 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,
  - une organisation administrative, comptable et informatique intègre et respectant les lois et standards applicables,
  - les principes directeurs en matière de sous-traitance (« outsourcing ») y compris de nature informatique reposant ou non sur une infrastructure de « cloud computing », 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 potentiellement non transparentes ;
- les principes directeurs en matière de continuité des activités et de gestion de crises ; et

- les principes directeurs régissant la nomination et la succession au conseil d'administration, à la direction autorisée et aux titulaires de fonctions clés de l'établissement, ainsi que les procédures régissant le conseil d'administration en termes de composition, comprenant les aspects de diversité, de responsabilités, d'organisation, de fonctionnement et d'évaluation individuelle et collective de ses membres.[3] Les aspects de diversité font référence aux caractéristiques des membres de l'organe de direction, y compris leur âge, sexe, origine géographique et parcours éducatif et professionnel. La promotion de la diversité repose sur le principe de non-discrimination et sur des mesures garantissant l'égalité des chances.

12. Le conseil d'administration charge la direction autorisée de mettre en œuvre les stratégies et principes directeurs par le biais de politiques et de procédures internes écrites (à l'exception des principes directeurs qui régissent la nomination et la succession au sein du conseil d'administration et les procédures déterminant son fonctionnement).

13. Le conseil d'administration surveille la mise en œuvre par la direction autorisée des stratégies et principes directeurs et approuve les politiques que la direction autorisée arrête en vertu de ces stratégies et principes.

14. Le conseil d'administration évalue d'une manière critique, adapte en cas de besoin et ré-approuve à des intervalles réguliers et au moins une fois par an, le dispositif de gouvernance interne, comprenant les stratégies clés et principes directeurs et leur implémentation au sein de l'établissement, les mécanismes de contrôle interne et le cadre de prise et de gestion des risques. Ces évaluations et ré-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 la ré-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 applicable, y compris la circulaire CSSF 11/506 ;

[3] 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.

- 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 de ses responsabilités et les performances de ses membres. Dans ce contexte, le conseil d'administration revoit et évalue d'une manière critique et constructive les actions, propositions, décisions de, et informations fournies par, la direction autorisée et 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, la CSSF et, le cas échéant, une autre autorité compétente ;
- 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, 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 potentiellement 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 spécialisés. Elles se font en particulier sur base des informations reçues de la part de la direction autorisée, 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 »), des rapports ICAAP/ILAAP et des rapports des fonctions de contrôle interne que le conseil d'administration est appelé à approuver à cette occasion.

15. Il appartient au conseil d'administration de promouvoir une culture interne en matière de risque et de compliance 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 et dans le cadre de politiques approuvées.

16. Le conseil d'administration veillera à consacrer un temps suffisant aux thématiques du risque.

17. 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 notifie 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 de membres du conseil d'administration ou de la direction autorisée ou d'un responsable d'une fonction clé.

Section 4.1.2. Composition et qualification du conseil d'administration

18. 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 qualités professionnelles (connaissances, compétences et expérience adéquates), ainsi qu'aux qualités personnelles des membres du conseil d'administration. Les qualités personnelles sont celles qui leur permettent d'exécuter leur mandat de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit requis. Par ailleurs, chaque membre doit justifier de son honorabilité professionnelle. Les principes directeurs régissant la nomination et la succession des membres du conseil d'administration expliquent et arrêtent les facultés jugées nécessaires en vue d'assurer une composition et une qualification appropriées du conseil d'administration.

19. Le conseil d'administration doit disposer collectivement de connaissances, compétences et d'une expérience appropriées à la nature, à l'échelle et à la complexité des activités et de l'organisation de l'établissement.

    Le conseil d'administration doit avoir collectivement 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.

20. Les membres du conseil d'administration veillent à ce que leurs qualités personnelles leur permettent d'exécuter leur mandat de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit 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 membres du personnel de l'établissement, à l'exception des représentants du personnel élus conformément à la réglementation applicable).

    Les membres du conseil d'administration veillent à ce que leur mandat soit et reste compatible avec leurs autres emplois, mandats 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.

21. 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 de membres existants doit s'orienter en particulier à leurs performances passées. La continuité du fonctionnement du conseil d'administration doit être assurée.

22. 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 une initiation spécifique pour comprendre la structure, le modèle d'affaires, le profil de risque et les dispositifs de gouvernance et ensuite des programmes de formation professionnelle qui permettent aux membres du conseil d'administration de comprendre d'une part, les opérations de l'établissement, leur rôle et d'autre part, de maintenir à jour et d'approfondir leurs compétences.

23. En principe, chaque entreprise d'investissement CRR devrait nommer au moins un membre à son conseil d'administration qui peut être considéré comme « membre indépendant ».

    Un membre indépendant du conseil administration ne connaît pas de conflits d'intérêts de nature à altérer sa capacité de jugement, du fait qu'il est, ou a été dans un passé récent, lié par une relation quelconque - professionnelle, familiale ou autre - avec l'établissement, l'actionnaire qui le contrôle ou la direction de l'un ou de l'autre. Pour l'appréciation du caractère d'indépendance, les établissements appliquent les critères de la section 9.3 des EBA/GL/2017/12 telle que reproduite en annexe I.

    Les établissements qui sont d'importance significative ou dont les actions sont admises à la négociation sur un marché réglementé veilleront à doter leur conseil d'administration d'un nombre suffisant de membres indépendants, compte tenu de leur organisation ainsi que de la nature, de l'échelle et de la complexité de leurs activités.

Section 4.1.3. Organisation et fonctionnement du conseil d'administration

24. Le conseil d'administration se réunit régulièrement en vue de s'acquitter de manière efficace de ses responsabilités. L'organisation et le fonctionnement du conseil d'administration sont consignés par écrit. Les objectifs et les responsabilités de ses membres sont également documentés par des mandats écrits.

25. Les travaux du conseil d'administration doivent être documentés par écrit. Cette documentation inclut l'agenda et les procès-verbaux des réunions avec les décisions et mesures prises par le conseil d'administration. Les procès-verbaux sont un outil important qui doit aider le conseil d'administration et ses membres à faire le suivi des décisions d'une part, et permettre au conseil d'administration et à ses membres de rendre des comptes aux actionnaires et à la CSSF d'autre part. Ainsi, des points de routine peuvent figurer de façon succincte sous forme de simple décision au procès-verbal d'une réunion, alors que des points importants de l'ordre du jour impliquant des risques pour l'établissement ou débattus contradictoirement doivent être rapportés plus en détail, permettant au lecteur de suivre les débats et d'identifier les positions défendues.

26. Le conseil d'administration évalue régulièrement les procédures régissant 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. Il veille à ce que tous ses membres aient une vision claire de leurs obligations, leurs responsabilités et de la répartition des tâches au sein du conseil d'administration et des comités spécialisés qui en dépendent.

27. Il appartient au président du conseil d'administration d'en assurer une composition équilibrée, notamment en termes de diversité, de veiller à son bon fonctionnement, de promouvoir au sein du conseil d'administration une culture de discussion informée et contradictoire et de proposer la nomination d'administrateurs indépendants. Le président du conseil d'administration n'exerce pas de fonctions exécutives au sein de l'établissement. Ainsi, les mandats de directeur autorisé et de président du conseil d'administration ne sont pas cumulables, et le président du conseil d'administration ne peut pas être un autre membre du personnel de l'établissement.

Section 4.1.4. Comités spécialisés

28. Le conseil d'administration peut se faire assister par des comités spécialisés dans les domaines notamment de l'audit, des risques, de la compliance, de la rémunération et des nominations ou encore de la gouvernance interne et de la déontologie, en fonction de ses besoins et compte tenu de l'organisation, de la nature, de l'échelle et de la complexité des activités de l'établissement. Les missions des comités spécialisés consistent à fournir au conseil d'administration des appréciations critiques concernant l'organisation et le fonctionnement de l'établissement dans leurs domaines de compétences spécifiques.

29. Les établissements d'importance significative doivent mettre en place un comité d'audit, un comité des risques, un comité de nomination et un comité de rémunération.

30. En application du principe de proportionnalité, les établissements qui ne sont pas d'importance significative peuvent mettre en place des comités dédiés combinant différents domaines de responsabilités, par exemple un comité d'audit et des risques, un comité d'audit et compliance ou encore un comité des risques et de rémunération. Les membres de tels comités combinés doivent posséder, individuellement et collectivement, les connaissances, les compétences et l'expertise nécessaires à l'exercice de leurs fonctions.

31. Sans préjudice d'exigences légales et réglementaires spécifiques en la matière, les membres permanents des comités spécialisés sont, selon le cas, des membres du conseil d'administration qui n'exercent pas de fonction exécutive au sein de l'établissement ou des membres indépendants. Chaque comité est composé d'au moins trois membres dont les connaissances, compétences et expertises sont en adéquation avec les missions du comité. Lorsqu'il existe au sein d'un établissement plusieurs comités spécialisés, l'établissement devrait, dans la mesure où le nombre de membres non-exécutifs et indépendants du conseil d'administration le permet, veiller à ce que les membres des comités respectifs soient différents. L'établissement devrait par ailleurs essayer d'assurer une rotation des présidents et membres des comités, compte tenu de l'expérience, des connaissances et des compétences spécifiques individuelles et collectives requises.

32. 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 et assurent un débat critique et constructif au sein du comité.

33. La CSSF recommande aux établissements d'importance significative que leur comité des risques comporte une majorité de membres indépendants, y compris son président.

34. Les comités spécialisés se réunissent régulièrement, afin de se décharger des tâches et travaux qui leur sont alloués ou encore pour préparer les réunions du conseil d'administration. Ils peuvent, suivant leurs besoins, se faire assister par des experts externes, indépendants de l'établissement, et peuvent associer à leurs travaux le réviseur d'entreprises agréé, les directeurs autorisés, les autres comités spécialisés, les responsables des fonctions de contrôle interne ainsi que d'autres personnes travaillant pour l'établissement, sans que ces personnes ne soient membres et sans qu'elles ne participent aux recommandations du comité.

35. Le conseil d'administration fixe par écrit les missions, la composition et les procédures de travail des comités spécialisés. En vertu de ces procédures, les comités spécialisés reçoivent des rapports réguliers des fonctions de contrôle interne sur l'évolution du profil de risque de l'établissement, les infractions par rapport au cadre réglementaire, à la gouvernance interne et à la gestion des risques ainsi que les préoccupations soulevées par l'intermédiaire du dispositif interne d'alerte et les mesures pour y remédier. Ils doivent pouvoir demander tout document et toute information qu'ils jugent utiles pour l'exercice de leur mission. Les comités documentent les agendas de leurs réunions ainsi que les conclusions et recommandations selon les mêmes principes qu'au point 25. Par ailleurs, les procédures prévoient les conditions dans lesquelles les experts externes fournissent leur assistance et les modalités selon lesquelles d'autres personnes sont associées aux travaux des comités spécialisés.

36. Le conseil d'administration veille à ce que les différents comités interagissent efficacement, communiquent entre eux et avec les fonctions de contrôle interne et le réviseur d'entreprises agréé et rapportent régulièrement au conseil d'administration.

37. Le conseil d'administration ne peut pas déléguer aux comités spécialisés ses pouvoirs et responsabilités en vertu de la présente circulaire. 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

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. Sans préjudice des autres dispositions de la section 4.1.4, les établissements doivent créer un comité d'audit lorsqu'ils y sont tenus par l'article 52 de la loi modifiée du 23 juillet 2016 relative à la profession de l'audit (« Loi Audit »).

40. Le comité d'audit est en charge du processus de nomination, de reconduction, de révocation[4] et de rémunération du réviseur d'entreprises agréé.

41. Le comité d'audit confirme la charte d'audit interne ainsi que le plan d'audit pluriannuel et ses révisions. 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 et l'indépendance nécessaires.

42. Le comité d'audit délibère régulièrement et de manière critique sur les sujets suivants[5] :
    - le respect des règles comptables et le processus d'élaboration de l'information financière ;
    - l'état du contrôle interne et le respect des règles fixées à ce sujet dans la présente circulaire, sur base notamment des rapports de la fonction d'audit interne ;
    - la qualité du travail réalisé par la fonction d'audit interne et le respect des règles fixées à ce sujet ;
    - la qualité du travail réalisé par le réviseur d'entreprises agréé, son indépendance et objectivité, son respect des règles déontologiques en vigueur ainsi que la portée et la fréquence d'audit. A ce titre, le comité d'audit analyse et évalue les rapports sur les comptes annuels, les « management letters », les comptes rendus analytiques et, le cas échéant, la nature appropriée des services autres que ceux liés à l'audit des comptes qui auraient été fournis par le réviseur d'entreprises agréé ;
    - 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 et les actions entreprises pour remédier aux problèmes, déficiences et irrégularités relevés.

43. En rendant compte au conseil d'administration dans son ensemble, le comité d'audit propose les mesures nécessaires pour corriger rapidement les problèmes, déficiences et irrégularités constatés. Le comité d'audit informe le conseil d'administration des conclusions de l'audit externe, de ses travaux pour s'assurer de l'intégrité du reporting légal et du rôle assumé par le comité d'audit dans ce processus.

[4] Le pouvoir de désignation du réviseur d'entreprises agréé appartient cependant au conseil d'administration de l'entreprise d'investissement conformément à l'article 22 de la LSF.

[5] 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.

Sous-section 4.1.4.2. Le comité des risques

44. Le comité des risques a pour objet de conseiller le conseil d'administration pour les aspects liés à la stratégie globale en matière de risques et d'appétit au risque et également de l'assister pour l'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.

45. Les établissements d'importance significative doivent créer un comité des risques, dans le respect des dispositions de l'article 7 du RCSSF 15-02.

46. Le comité des risques confirme les politiques spécifiques de la direction autorisée suivant la section 1.1.2 de la partie III. Il assiste le conseil d'administration dans sa mission de surveillance de la mise en application de la stratégie en matière de risques, du cadre global de prise et de gestion des risques et de l'adéquation de l'ensemble des risques encourus en lien avec la stratégie, l'appétit au risque et les mesures d'atténuation de risque de l'établissement.

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

48. Le comité des risques conseille et assiste le conseil d'administration en ce qui concerne le recrutement d'experts externes que le conseil d'administration se proposerait d'engager pour apporter du conseil ou du support.

49. Le comité des risques délibère régulièrement et de manière critique sur les sujets suivants :
    - le profil de risque de l'établissement, son évolution en conséquence d'événements internes et externes, son adéquation avec la stratégie approuvée en matière de risques, l'appétit aux risques, les politiques et systèmes de limites en matière de risques ainsi que la capacité de l'établissement à gérer et à supporter ces risques sur une base continue compte tenu de ses fonds propres et réserves de liquidités internes et réglementaires ;
    - l'adéquation du cadre de prise et de gestion des risques avec la stratégie et les objectifs commerciaux, la culture d'entreprise et le cadre de valeurs de l'établissement ;
    - 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 ;
    - l'évaluation, par le biais de scénarios et de tests d'endurance, de l'influence d'événements externes et internes sur le profil de risque de l'établissement et de la capacité de l'établissement à supporter ses risques ;

- le suivi approprié et sans délai indu par la direction autorisée, des recommandations de la fonction de contrôle des risques et les actions entreprises pour remédier aux problèmes, déficiences et irrégularités relevés ;
- la conformité et la tarification des produits et services clés offerts aux clients avec le modèle d'affaires et la stratégie approuvée en matière de risques ;
- sans préjudice des responsabilités du comité de rémunération, le caractère approprié des avantages prévus dans les politiques et pratiques de rémunération, compte tenu du niveau de risques de l'établissement, de ses fonds propres et de ses réserves de liquidités internes et réglementaires ainsi que de sa profitabilité.

Le comité des risques rend compte au conseil d'administration dans son ensemble du résultat de ses délibérations en proposant les mesures nécessaires pour corriger rapidement les problèmes, déficiences et irrégularités constatés.

50. Le président du comité des risques ne peut être en même temps président du conseil d'administration ni d'aucun autre comité spécialisé.

Sous-chapitre 4.2. La direction autorisée

Section 4.2.1. Responsabilités de la direction autorisée

51. La direction autorisée est responsable de 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 approuvés par le conseil d'administration et de la réglementation applicable, en prenant en considération et en préservant les intérêts financiers de l'établissement à long terme, sa solvabilité et sa situation des liquidités. La direction autorisée évalue de façon constructive et critique toutes les propositions, explications et informations qui lui sont soumises pour décision. La direction autorisée documente ses décisions à l'aide de procès-verbaux de réunions, qui doivent l'aider à faire le suivi des décisions prises d'une part, et lui permettre de rendre compte de sa gestion au conseil d'administration et à la CSSF d'autre part. Ainsi, des points de routine peuvent figurer de façon succincte sous forme de simple décision au procès-verbal d'une réunion, alors que des points importants de l'ordre du jour impliquant des risques pour l'établissement ou débattus contradictoirement doivent être rapportés plus en détail, permettant au lecteur de suivre les débats et d'identifier les positions défendues.

52. Conformément à l'article 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 qu'au moins un membre de la direction autorisée en fasse partie et qu'il existe un droit de veto à son bénéfice.

53. 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.

    La direction autorisée veille à ce que l'établissement dispose des 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 des principes directeurs en matière de déontologie, de valeurs d'entreprise et de gestion des conflits d'intérêts arrêtés par le conseil d'administration, 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.

    L'objectif de ce code de conduite doit être la prévention des risques opérationnels et de réputation dont l'établissement pourrait souffrir du fait de sanctions administratives ou pénales, de mesures restrictives à son encontre ou de litiges juridiques, de la perte de son image de marque ou de la confiance de ses clients et des consommateurs. Le code de conduite devrait rappeler au personnel, aux directeurs autorisés et aux membres du conseil d'administration le respect de la réglementation applicable, des règles et limites internes, des principes sous tendant un comportement honnête et intègre aussi bien que les cas de conduite inappropriée et les mesures de sanction qui en découleraient.

56. La direction autorisée doit avoir une compréhension parfaite de la structure organisationnelle et opérationnelle de l'établissement, en particulier en termes d'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 entités 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 de la fonction compliance.

    La direction autorisée met en œuvre de manière prompte et efficace les mesures correctrices pour remédier aux faiblesses (problèmes, déficiences, irrégularités ou préoccupations) relevées par les fonctions de contrôle interne, le réviseur d'entreprises agréé ou par l'intermédiaire du dispositif d'alerte interne en prenant en compte les recommandations émises dans ce contexte. 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 des délais d'implémentation des 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.

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 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 (y compris les préoccupations soulevées par l'intermédiaire du dispositif d'alerte interne) et celui du contrôle interne, ainsi que les rapports ICAAP/ILAAP sur la situation et la gestion des risques, des fonds propres et des réserves de liquidités réglementaires et internes.

62. 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.

63. 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.

64. Nonobstant la responsabilité collective des membres de la direction autorisée, 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. Ce membre est responsable en particulier de l'établissement de l'organigramme et de la description des tâches qu'il soumet, avant leur mise en application, à l'approbation de la direction autorisée. Il veille ensuite à leur application correcte. Le membre en question est aussi responsable de la production et de la publication des informations comptables destinées aux tiers et de la communication des informations périodiques à la CSSF. Il veillera donc à ce que la forme et le contenu de ces informations soient conformes aux prescriptions légales et aux instructions 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.

65. Les établissements informent la CSSF des nominations et révocations des membres de la direction autorisée, conformément aux dispositions de la présente circulaire et de la Procédure prudentielle, en communiquant par ailleurs les motifs expliquant la révocation.

Section 4.2.2. Qualification de la direction autorisée

66. Les membres de la direction autorisée possèdent, à la fois individuellement et collectivement, les qualités professionnelles (connaissances, compétences et expérience adéquates), l'honorabilité professionnelle 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 d'esprit requis.

Chapitre 5. Organisation administrative, comptable et informatique

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

67. 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. L'organigramme et la description des tâches sont arrêtés par écrit et mis à la disposition de l'ensemble du personnel concerné sous une forme facilement accessible.

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

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

70. 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.

71. Conformément à l'article 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 déroge pas à cette responsabilité conjointe. Cette dernière reste compatible avec la pratique suivant laquelle les membres de la direction autorisée se répartissent les tâches journalières du suivi rapproché des différentes activités. L'établissement doit organiser cette répartition de manière à éviter les conflits d'intérêts. Ainsi, un même membre de la direction autorisée ne peut se voir attribuer la charge ou la responsabilité à la fois de fonctions de prise de risque et de contrôle indépendant de ces mêmes risques. De même, le directeur autorisé, qui assume lui-même le poste de « Chief Risk Officer » et/ou le poste de « Chief Compliance Officer » suivant le point 134 et/ou le point 148 de cette partie, ne peut pas en même temps être en charge de la fonction d'audit interne (voir les incompatibilités des fonctions dans l'encadré ci-dessous). 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.

Incompatibilités des fonctions :

Le directeur autorisé, qui assume lui-même le poste de « Chief Compliance Officer » et/ou de « Chief Risk Officer » indépendamment du fait qu'il est le membre de la direction autorisée en charge de la fonction Compliance et/ou le membre de la direction autorisée en charge de la fonction de contrôle des risques, ne peut pas être en même temps le membre de la direction autorisée en charge de la fonction d'audit interne et/ou le « Chief Internal Auditor ».

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

73. Chaque membre du personnel doit prendre annuellement au moins deux semaines calendaires consécutives de congés personnels. Il doit être assuré que chaque membre du personnel soit effectivement absent pendant ce congé et que son remplaçant prenne effectivement en charge le travail de la personne absente.

Sous-chapitre 5.2. Les procédures et la documentation interne

74. 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 un manuel des procédures clair, complet, détaillé et accessible dont les procédures sont connues de l'ensemble du personnel concerné et qui est tenu à jour en continu.

75. La description des procédures pour assurer l'exécution correcte des activités porte sur les points suivants :

    - les étapes successives et logiques du traitement des opérations, de leur initiation à l'archivage de leur documentation (« workflow ») ;
    - les contrôles à réaliser, ainsi que les moyens pour s'assurer que ceux-ci ont été réalisés.

76. 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.

77. 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 de cette partie ainsi que les rapports de révision établis par le réviseur d'entreprises agréé sont conservés pendant au moins cinq ans, sans préjudice d'autres législations applicables, 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.

78. 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.

Commission de Surveillance du Secteur Financier

Sous-chapitre 5.3. L'infrastructure administrative et technique

79. L'établissement se dote des fonctions de support, des moyens matériels et techniques nécessaires et suffisants à l'exécution de ses activités.

Section 5.3.1. L'infrastructure administrative des fonctions commerciales

80. 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 5.3.2. La fonction financière et comptable

81. L'établissement dispose d'un service comptable et financier dont la mission est d'assumer la gestion comptable et financière 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.

    Dans les établissements d'importance significative, le CFO est sélectionné, nommé et révoqué suivant une procédure interne écrite, avec approbation au préalable par le conseil d'administration.

82. 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, d'expositions de crédits non performants, de crédits restructurés 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 la prise de décisions informées et 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.

83. 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.

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

85. 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.

86. 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 de leur nécessité.

    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.

87. 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 par le service comptable et financier.

88. 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 afin d'éviter en particulier que le système comptable ne puisse être utilisé à des fins frauduleuses.

Section 5.3.3. La fonction informatique

89. 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 chapitre 3 de cette partie. Pour ce faire, ils respectent les exigences de la circulaire CSSF 20/750 relative aux exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité.

90. Les établissements qui, en matière de fonction informatique, recourent aux services de tiers respectent en particulier les conditions définies au sous-chapitre 7.4 de cette partie.

Section 5.3.4. Le dispositif de communication et d'alerte interne et externe

91. 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.

92. 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.

93. 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 légitimes liées à la gouvernance interne ou aux exigences internes et réglementaires en général. Ce dispositif respecte la confidentialité de l'identité 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 ou retombée défavorable d'aucune sorte dans le chef des personnes qui les ont données.

94. La CSSF met également à disposition sur son site internet un outil et une procédure permettant la déclaration d'incidents directement à la CSSF. (https://whistleblowing.apps.cssf.lu/index.html?language=fr).

Section 5.3.5. Le dispositif de gestion de crises

95. 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.

96. Le dispositif de gestion de crises comprend, le cas échéant, un plan de redressement qui est conforme aux exigences du chapitre 2 de la partie IV de la LSF.

97. 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.

Chapitre 6. Le contrôle interne

98. Le contrôle interne est un dispositif composé de règles et de procédures qui ont pour but de s'assurer que les objectifs posés par l'établissement sont atteints, que les ressources sont utilisées de façon efficiente, que les risques sont contrôlés et que le patrimoine est protégé, que l'information financière et l'information de gestion sont correctes, complètes, pertinentes, compréhensibles et disponibles sans délais, que les lois et réglementations ainsi que les politiques et les procédures internes sont respectées, que les demandes et exigences de la CSSF sont respectées[6].

99. Le dispositif de contrôle interne d'un établissement doit être adapté à son organisation et à la nature, à l'échelle et à la complexité de ses activités et des risques associés et respecter les principes du modèle des « trois lignes de défense » :

    La première ligne de défense est constituée par les unités opérationnelles qui prennent ou acquièrent des risques, qui assument la responsabilité pour leur gestion et qui contrôlent de manière permanente le respect des politiques, procédures et limites qui leur sont imposées.

    La seconde ligne est formée par des fonctions de support, comme la fonction financière et comptable, mais surtout les fonctions compliance et de contrôle des risques, qui assurent un contrôle indépendant des risques et supportent les unités opérationnelles dans le respect des politiques et procédures qui leur sont applicables.

    La troisième ligne est constituée par la fonction d'audit interne qui effectue une évaluation indépendante, objective et critique des deux premières lignes de défense et du dispositif de gouvernance interne dans son ensemble.

    Les trois lignes de défense sont complémentaires, chaque ligne de défense assumant ses responsabilités de contrôle indépendamment des autres lignes.

    La mise en place d'un dispositif de contrôle interne solide va de pair avec une séparation pertinente des fonctions, tâches et responsabilités, la mise en place d'une gestion des accès à l'information et la séparation physique de certaines fonctions et de certains départements afin de sécuriser les données et les transactions.

[6] 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 tenue de comptabilité et du calcul de la valeur nette d'inventaire de fonds d'investissement.

Sous-chapitre 6.1. Les contrôles opérationnels

Un environnement de contrôle interne solide comporte les types de contrôles suivants :

Section 6.1.1. Contrôles quotidiens réalisés par le personnel exécutant

100. 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 caisse, la vérification de ses positions par le trader, le suivi de ses suspens par chaque membre du personnel.

Section 6.1.2. Contrôles critiques continus

101. 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 ;
- les contrôles réciproques ;
- le relevé régulier de l'existence et de la valeur des éléments du patrimoine, notamment au moyen de la vérification des inventaires ;
- la réconciliation et la confirmation des comptes ;
- le contrôle de l'exactitude et de l'exhaustivité des données communiquées par les personnes en charge des fonctions commerciales et opérationnelles en vue d'un suivi administratif des opérations ;
- le contrôle du respect des limites internes imposées par la direction autorisée ;
- 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

102. 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 les membres de la direction autorisée 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 ;
- 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 les autres membres de la direction autorisée sur l'exercice de leur mission de contrôle.

Sous-chapitre 6.2. Les fonctions de contrôle interne

103. Les politiques mises en œuvre en matière de contrôle des risques, de compliance et d'audit interne 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. 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 afin d'éviter les redondances et conflits de compétences, et définissent les objectifs ainsi que l'indépendance, l'autorité, l'objectivité et la permanence des fonctions de contrôle interne.

Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne

104. Les fonctions de contrôle interne ont pour objectif principal de vérifier le respect de l'ensemble des politiques et des 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 et, le cas échéant, aux comités spécialisés. Elles fournissent à la direction autorisée ainsi qu'au conseil d'administration et, le cas échéant, aux comités spécialisés les avis et conseils qu'elles jugent utiles ou qui leur sont demandés par ces organes ou comités.

105. Lorsqu'ils 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.

106. Lorsque l'établissement est tête de groupe, ses fonctions de contrôle interne surveillent et contrôlent les fonctions de contrôle interne des différentes entités du groupe. Les fonctions de contrôle interne de l'établissement veillent à ce que les problèmes, déficiences, irrégularités et risques relevés à travers l'ensemble du groupe soient rapportés aux organes de direction et de surveillance locaux ainsi qu'à la direction autorisée et au conseil d'administration de tête de groupe.

Section 6.2.2. Caractéristiques des fonctions de contrôle interne

107. 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 aux comités spécialisés le cas échéant, 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 ;
- 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 ;
- 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 ;

- les responsables des fonctions de contrôle interne sont subordonnés aux personnes en charge de, ou responsables pour, les activités que les fonctions de contrôle internes sont appelées à contrôler.

108. 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) qu'elles jugent nécessaires pour l'accomplissement de leurs missions.

109. Les fonctions de contrôle interne ou les tiers 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 ; elles ne doivent pas subordonner leur propre jugement à celui d'autres personnes, dont surtout les personnes contrôlées, et veillent à éviter les conflits d'intérêts.

110. Les membres des fonctions de contrôle interne doivent posséder un niveau individuel et collectif des connaissances, des compétences et une expérience professionnelles élevées dans le domaine des activités financières et plus particulièrement dans leur domaine de responsabilités en ce qui concerne les normes applicables. Conformément au principe de proportionnalité, le niveau de compétences requis augmente en fonction de l'organisation de l'établissement et de la nature, de l'échelle et de la complexité des activités et des risques. La 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 des connaissances théoriques nécessaires.

111. 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. Le budget doit être suffisamment flexible pour tenir compte d'une adaptation des missions des fonctions de contrôle interne en réponse à des changements au niveau de l'organisation, des activités et des risques de l'établissement ou en cas de survenance d'événements spécifiques.

112. 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 potentiellement non transparentes.

113. 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

114. 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.

115. Les fonctions de contrôle interne rapportent par écrit régulièrement et si nécessaire sur base ad hoc à la direction autorisée et au conseil d'administration ou, le cas échéant, aux comités spécialisés. Ces rapports portent sur le suivi des recommandations, 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 couvrant l'ensemble des activités qui lui sont attribuées. Au titre des activités, chaque rapport de synthèse fournit le relevé des activités de la fonction depuis le dernier rapport, des principales recommandations adressées à la direction autorisée, des problèmes (existants ou émergents), déficiences et irrégularités majeures survenus depuis le dernier rapport, des mesures prises à leur égard ainsi que le relevé des problèmes, déficiences et irrégularités relevés dans le dernier rapport mais qui n'ont pas encore fait l'objet de mesures correctrices appropriées. 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 l'adéquation des ressources humaines et techniques internes et la nature et le degré du recours à des ressources humaines et techniques externes ainsi que sur les problèmes éventuels apparus dans ce contexte. Ce rapport est soumis pour approbation au conseil d'administration ou aux comités spécialisés compétents pour en assurer le suivi et l'information au conseil d'administration ; il est soumis pour information à la direction autorisée.

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, le cas échéant, les présidents des comités spécialisés. Dans ces cas, les responsables des fonctions de contrôle interne peuvent demander à être 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 de cette partie. Elles rapportent de manière régulière à ce sujet à la direction autorisée.

Section 6.2.4. Organisation des fonctions de contrôle interne

116. Chaque fonction de contrôle interne est placée sous la responsabilité d'un chef de fonction distinct qui est sélectionné, nommé et révoqué suivant une procédure interne écrite. Les nominations et révocations des responsables des fonctions de contrôle interne sont approuvées au préalable par le conseil d'administration et rapportées par écrit à la CSSF dans le respect de la Procédure prudentielle telle que publiée par la CSSF sur son site internet.

117. 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 directement et de leur propre initiative le président du conseil d'administration ou, le cas échéant, le comité spécialisé compétent.

Les responsables des trois 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.

118. Une sous-traitance de la fonction compliance et de la fonction de contrôle des risques n'est pas admise.

Il est admissible que les tâches opérationnelles de la fonction d'audit interne soient sous-traitées par de petits établissements dont le profil de risque est faible et non complexe. Une telle sous-traitance n'est en principe pas acceptable dans le cas d'établissements qui ont des agences, des succursales ou des filiales.

Le conseil d'administration de l'établissement conserve la responsabilité finale pour la sous-traitance des tâches opérationnelles de l'audit interne. Les prestataires externes auxquels les tâches opérationnelles de l'audit interne sont sous-traitées dépendent et rapportent directement au membre de la direction autorisée en charge de l'audit interne. Ils ont également un accès direct au conseil d'administration ou, le cas échéant, au président du comité d'audit.

119. Les dispositions du point précédent n'excluent pas que les fonctions de contrôle interne aient recours à l'expertise et aux ressources humaines ou techniques de tiers (faisant partie du même groupe que l'établissement ou non) 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 ressources externes.

La direction autorisée sélectionne ces ressources externes sur base d'une analyse d'adéquation entre les besoins de l'établissement et les services, le niveau d'objectivité et d'indépendance et les compétences spécifiques offerts par ces tiers, qui doivent être indépendants du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent. Le conseil d'administration approuve les ressources externes sélectionnées par la direction autorisée.

120. Tout recours à des ressources externes doit se faire sur base d'un mandat écrit. Ces tiers réalisent leurs travaux dans le respect des dispositions réglementaires et internes qui sont applicables à la fonction de contrôle interne et au domaine de contrôle en question. Ils doivent être placés sous la dépendance du responsable de la fonction de contrôle interne dont relève le domaine contrôlé. Ce responsable supervise les travaux de ces tiers.

121. Lorsqu'en application du principe de proportionnalité, l'établissement peut démontrer qu'il n'est pas justifié de mettre en place une fonction de contrôle des risques et une fonction compliance distinctes ou de nommer deux responsables à temps plein à la tête de ces deux fonctions, l'établissement peut soit mettre en place une fonction combinée ou un poste à responsabilité combinée, soit charger deux personnes distinctes à temps partiel, moyennant l'accord préalable de la CSSF.

L'établissement qui désire créer une fonction combinée de contrôle des risques et de compliance, cumuler les responsabilités pour ces deux fonctions dans le chef d'une seule personne ou combiner l'une de ces responsabilités avec d'autres tâches ou charger deux personnes distinctes à temps partiel, doit adresser une demande à la CSSF qui comprendra :

- soit une description de la fonction combinée ou du poste à responsabilité combinée, soit une description des fonctions des deux personnes chargées à temps partiel ;
- une description de toutes les autres tâches exercées par la (les) personne(s) en question ;
- l'analyse et ses conclusions justifiant soit la création d'une fonction combinée ou d'un poste à responsabilité combinée, soit le fait de charger deux personnes distinctes à temps partiel, au vu de l'organisation de l'établissement, de la nature, de l'échelle et de la complexité de ses activités et risques ;
- la décision du conseil d'administration approuvant l'analyse et ses conclusions ; et
- une confirmation écrite que les autres tâches exercées par la (les) personne(s) en question restent compatibles avec les responsabilités susvisées.

122. L'établissement qui, en application du principe de proportionnalité, désire sous-traiter les tâches opérationnelles de la fonction d'audit interne doit adresser une demande préalable à la CSSF qui comprendra :
- l'analyse et ses conclusions justifiant la sous-traitance des tâches opérationnelles de la fonction d'audit interne ;
- la décision du conseil d'administration approuvant l'analyse et ses conclusions et, le cas échéant, l'avis du comité d'audit ;
- une description de la sous-traitance, le prestataire retenu, les ressources externes contractées et le nom du responsable de l'équipe externe devant assurer les missions d'audit interne ; et
- la personne responsable de cette sous-traitance au sein de l'établissement.

Ces prestataires externes peuvent être les auditeurs internes du groupe dont fait partie l'établissement. Il appartient au conseil d'administration de s'assurer que ces ressources sont suffisantes et disposent de l'expérience et des compétences nécessaires pour couvrir tous les domaines d'activités de l'établissement et les risques liés ainsi que de l'encadrement requis pour assurer un travail d'audit de haute qualité.

123. 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.

124. Pour les succursales, les fonctions de contrôle interne dépendent, d'un point de vue hiérarchique et fonctionnel, des fonctions de contrôle des entités juridiques 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 la tête de groupe. Les rapports établis conformément aux dispositions de la présente circulaire sont soumis non seulement à la direction autorisée et au conseil d'administration local, 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 115.

En vertu du principe de proportionnalité, l'établissement qui a créé trois fonctions de contrôle interne permanentes et indépendantes peut renoncer à mettre en place auprès d'entités juridiques ou de succursales du groupe dont la taille et les activités sont limitées, des fonctions de contrôle interne propres. Dans ce cas, l'établissement veille à ce que ses fonctions de contrôle interne procèdent à des contrôles réguliers et fréquents, y compris des contrôles sur place annuels, auprès de ces entités.

Lorsque l'établissement n'est pas entreprise mère, 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 115.

125. 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

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

126. La fonction de contrôle des risques s'assure que toutes les unités opérationnelles anticipent, détectent, évaluent, mesurent, suivent, gèrent et déclarent dûment tous les risques auxquels l'établissement est ou pourrait être exposé. Elle réalise ses tâches de manière continue et sans délais. Elle est un élément central de la gouvernance interne et de l'organisation de l'établissement qui est dédié à la maîtrise des risques. Elle informe et conseille le conseil d'administration et assiste la direction autorisée, propose des améliorations au cadre de gestion des risques et participe activement aux processus de décisions en veillant à ce qu'une attention appropriée soit accordée aux considérations de risque. La responsabilité ultime pour les décisions en matière de risque reste cependant auprès des unités opérationnelles qui prennent les risques et, en fin de compte, auprès de la direction autorisée et du conseil d'administration. Le terme fonction de contrôle des risques n'entend donc pas réduire cette fonction à un simple « contrôle » ex-post de limites.

127. Le champ d'intervention de la fonction de contrôle des risques couvre l'établissement dans son ensemble, y compris les risques inhérents à la complexité de la structure juridique de l'établissement et aux relations de l'établissement avec des parties liées.

128. La fonction de contrôle des risques veille à ce que les objectifs et limites internes en matière de risque soient robustes et compatibles avec le cadre réglementaire, les stratégies et politiques internes, les activités et la structure organisationnelle et opérationnelle de l'établissement. Elle en contrôle le respect, propose des mesures de remédiation appropriées en cas d'infraction, veille au respect de la procédure d'escalade en cas d'infraction matérielle et s'assure que les dépassements soient régularisés dans les meilleurs délais.

129. Le responsable de la fonction de contrôle des risques veille à ce que la direction autorisée et le conseil d'administration reçoivent une vue indépendante, 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 et 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 l'appétit au risque défini par le conseil d'administration. La fréquence de cette communication est adaptée aux caractéristiques et aux besoins de l'établissement, compte tenu de son modèle d'affaires, des risques encourus et de son organisation.

Le rapport annuel de synthèse de la fonction de contrôle des risques, qui est fourni en copie à la CSSF, fait potentiellement double emploi avec des éléments du rapport ICAAP et ILAAP. La fonction de contrôle des risques peut dès lors faire référence dans son rapport de synthèse au rapport ICAAP et ILAAP pour autant qu'elle partage les descriptifs et analyses de risques qui y figurent. En cas de désaccord, la fonction de contrôle des risques émet dans son rapport de synthèse ses propres évaluations et conclusions.

130. 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.

131. La fonction de contrôle des risques veille à ce que l'appréciation 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 méthodes d'appréciation qualitatives et des jugements d'experts, basés sur des analyses structurées et documentées.

La fonction de contrôle des risques informe la direction autorisée et le conseil d'administration sur les hypothèses, les limites et les déficiences potentielles des analyses et modèles appliqués et doit régulièrement confronter ses appréciations ex-ante des risques potentiels mesurés avec les risques matérialisés ex-post en vue d'améliorer la justesse de ses méthodes d'appréciation (« back-testing »).

132. 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 (« New Product Approval Process ») 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

133. Les établissements créent une fonction de contrôle des risques permanente et indépendante compte tenu du principe de proportionnalité et des critères régissant son application, ainsi que des considérations sur l'organisation des fonctions de contrôle interne élaborées à la section 6.2.4. Lorsque l'organisation d'un établissement, l'ampleur ou la complexité de ses activités ou encore les risques encourus justifient la mise en place de fonctions satellites de contrôle des risques ou compliance au sein des unités opérationnelles, l'établissement doit néanmoins mettre en place une fonction centrale de contrôle des risques à laquelle rapportent les différentes fonctions satellites. Cette fonction centrale gère la vue consolidée des risques et s'assure du respect des stratégies et de l'appétit définis en matière de risques.

134. 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 de contrôle des risques assume lui-même le poste de « Chief Risk Officer ».

135. Au sein des établissements qui sont d'importance significative, le responsable de la fonction de contrôle des risques est un membre de la direction autorisée qui est indépendant et individuellement responsable de la fonction de contrôle des risques. Lorsque le principe de proportionnalité n'exige pas une telle attribution, et en l'absence de conflits d'intérêts, un autre membre du personnel de l'établissement faisant partie de l'encadrement supérieur peut assumer cette fonction.

136. Le responsable de la fonction de contrôle des risques doit être en mesure de contester les décisions de la direction autorisée. Ces contestations et les raisons invoquées doivent être documentées par l'établissement. Lorsque l'établissement accorde au « Chief Risk Officer » un droit de veto sur les décisions de la direction autorisée, la portée de ce droit doit être arrêtée clairement et par écrit, y compris le processus d'escalade au conseil d'administration.

Les décisions ayant fait l'objet d'un avis négatif motivé de la part du « Chief Risk Officer » devraient être sujettes à un processus décisionnel renforcé.

Section 6.2.6. La fonction compliance

La présente circulaire comprend les « orientations générales » contenues dans les orientations de l'ESMA concernant certains aspects de la MiFID relatifs aux exigences de la fonction de vérification de la conformité (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 les ESMA/2012/388.

Sous-section 6.2.6.1. La charte de compliance

137. 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.

138. 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 clés (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 et 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 et filiales au Luxembourg et à l'étranger.

139. La charte de compliance doit être mise à jour dans les meilleurs délais pour tenir compte de changements au niveau des normes applicables 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. Champ d'application et responsabilités spécifiques de la fonction compliance

140. La fonction compliance a pour objectif d'anticiper, de détecter, d'évaluer, de déclarer et de suivre les risques de compliance d'un établissement ainsi que d'assister la direction autorisée à doter l'établissement de mesures pour se conformer aux lois, règlements et standards applicables. Les risques de compliance 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 d'autres aspects du risque opérationnel, ceci en relation avec l'intégralité des activités de l'établissement.

Ces tâches sont à réaliser continuellement et sans délais.

141. Pour atteindre les objectifs fixés, les responsabilités de la fonction compliance doivent couvrir au moins les aspects suivants :

- la fonction compliance identifie les normes auxquelles l'établissement est soumis dans l'exercice de ses activités dans les différents marchés et tient le relevé des règles essentielles. Ce relevé doit être accessible au personnel concerné de l'établissement ;
- la fonction compliance identifie les risques de compliance auxquels l'établissement est exposé dans le cadre de l'exercice de ses activités et en évalue l'importance et les conséquences possibles. Le classement des risques de compliance ainsi déterminé doit permettre à la fonction compliance d'établir son plan de contrôle en fonction du risque, permettant ainsi une utilisation efficace des ressources de la fonction compliance ;
- la fonction compliance veille à l'identification et l'évaluation du risque de compliance avant que l'établissement ne se lance dans un nouveau type d'activité, de produit ou de relation d'affaires, de même que lors du développement des opérations et du réseau d'un groupe sur une échelle internationale (« New Product Approval Process ») ;
- 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 leurs 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 et tiennent compte du code de conduite et des valeurs d'entreprise dont s'est doté l'établissement ;
- les domaines qui relèvent directement de la fonction compliance sont typiquement la lutte contre le blanchiment de capitaux et le financement du terrorisme, les services d'investissement, la prévention en matière d'abus de marché et de transactions personnelles, les fraudes, la protection des intérêts et des données des clients et la prévention et la gestion des conflits d'intérêts. Cette liste n'est pas exhaustive et il appartient à l'établissement de décider si sa fonction compliance couvre également le respect d'autres règles que celles énoncées ci-avant ;

- le « Chief Compliance Officer » veille en particulier à ce que la lutte contre le blanchiment de capitaux et le financement du terrorisme se traduise par des mesures et contrôles efficaces et appropriés au risque. Le rapport de synthèse de la fonction compliance adressé en copie à la CSSF couvrira le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme par un chapitre dédié relatant les activités et événements liés au domaine concerné, c'est-à-dire les principales recommandations émises, les déficiences, irrégularités et problèmes majeurs (existants ou émergents) constatés, les mesures correctrices et préventives mises en place ainsi qu'un relevé des déficiences, irrégularités et problèmes qui n'ont pas encore fait l'objet de mesures correctrices appropriées ;
- d'une manière générale, la fonction compliance est à organiser de façon à couvrir tous les domaines pouvant donner lieu à des risques de compliance. Il est admissible que les domaines autres que ceux énumérés ci-dessus ne soient pas directement couverts par la fonction compliance. 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 de l'information et de vérification que les autres domaines ne relevant pas directement de son champ d'intervention sont bien couverts.

142. 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 dans le cadre d'un programme de contrôle structuré. 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.

143. La fonction compliance centralise toutes les informations sur les problèmes de compliance (entre autres les fraudes internes et externes, les infractions aux normes, le non-respect de procédures et de limites 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 d'entreprises agréé, correspondance de la part de la CSSF ou d'autres autorités compétentes).

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

145. 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.

146. Le « Chief Compliance Officer » est la personne de contact privilégiée des autorités compétentes en matière de lutte contre le blanchiment de capitaux 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

147. Les établissements créent une fonction compliance permanente et indépendante compte tenu du principe de proportionnalité et des critères régissant son application, ainsi que des considérations générales sur l'organisation des fonctions de contrôle interne élaborées à la section 6.2.4.

148. 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

Sous-section 6.2.7.1. La charte d'audit interne

149. 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 clés (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 ses succursales et filiales au Luxembourg et à l'étranger ainsi que les activités et fonctions faisant l'objet d'une sous-traitance, à accéder à tous les documents, pièces, procès-verbaux des organes consultatifs et décisionnels de l'établissement, à voir toutes les personnes travaillant pour 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 les standards professionnels reconnus qui gouvernent le fonctionnement et les travaux de l'audit interne [7] ;
- 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 et 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.

[7] *Tel que par exemple le « International Professional Practices Framework (IPPF) » de l'Institute of Internal Auditors (IIA).*

150. 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. 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

151. La fonction d'audit interne examine et évalue, entre autres (liste non exhaustive[8]), en fonction de l'organisation et de la nature, de l'échelle et de la complexité des activités :

- le suivi du respect des lois et réglementations ainsi que des exigences prudentielles imposées par la CSSF ;
- l'efficacité et l'efficience du dispositif en matière d'administration centrale, de gouvernance et de contrôle interne, en ce compris la fonction de contrôle des risques et la fonction compliance ;
- 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 ;

[8] *Le principe 7 du document « BCBS_223 The internal audit function in banks » contient une liste plus complète des activités qui peuvent rentrer dans le champ d'application de la fonction d'audit interne des établissements.*

- le respect des politiques et procédures, en particulier celles régissant l'adéquation des fonds propres et des réserves de liquidités internes ;
- l'adéquation de la gestion des risques ;
- l'intégrité des processus devant assurer la fiabilité des méthodes et outils utilisés par l'établissement, les hypothèses et données utilisées dans les modèles internes, les outils qualitatifs servant à l'identification et l'évaluation des risques ainsi que les mesures d'atténuation du risque qui sont prises ;
- le fonctionnement et l'efficacité des fonctions compliance et de contrôle des risques.

152. 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.

153. La mise en place d'une fonction d'audit interne locale 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 locales.

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

154. 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 et de l'efficacité de l'organisation et du contrôle interne en vigueur pour cette activité ou fonction (approche basée sur le risque). Le plan tient compte des avis du conseil d'administration ou 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.

155. Le plan est discuté avec la direction autorisée et 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 en fonction des développements et des urgences. Toute adaptation est à revoir par la direction autorisée et le comité d'audit, le cas échéant, avant d'être approuvée par le conseil d'administration. 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, 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.

156. Le plan 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.

Le plan d'audit interne prévoit une couverture adéquate des domaines présentant un risque de blanchiment de capitaux ou de financement du terrorisme de manière à permettre à l'audit interne de rendre compte annuellement dans le rapport de synthèse sur le respect de la conformité à la politique de lutte contre le blanchiment de capitaux ou de financement du terrorisme.

157. 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 est recommandé 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.

158. 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.

159. 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.

160. Chaque mission doit faire l'objet d'un rapport écrit du service d'audit interne destiné 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). 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.

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

161. Les établissements créent une fonction d'audit interne permanente et indépendante compte tenu du principe de proportionnalité et des critères régissant son application, ainsi que des considérations sur l'organisation des fonctions de contrôle interne élaborées à la section 6.2.4.

162. En cas de sous-traitance des tâches opérationnelles de l'audit interne, les prestataires externes réalisent leurs travaux dans le cadre du plan d'audit interne de l'établissement, en suivant un programme de travail, en documentant leurs 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 responsable désigné de la fonction, à la direction autorisée, au comité d'audit, le cas échéant, et au conseil d'administration. Lorsque ces prestataires externes 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 »)

163. La structure organisationnelle, en termes d'entités (structures) juridiques, est appropriée et justifiée par rapport aux stratégies et principes directeurs. Elle est claire et transparente aux yeux de l'ensemble des parties prenantes.

La structure juridique, organisationnelle et opérationnelle doit permettre et promouvoir une gestion efficace, saine et prudente des activités. Elle ne doit pas entraver la bonne gouvernance de l'établissement, en particulier la capacité de l'organe de direction à gérer et à contrôler efficacement les activités (et les risques) de l'établissement et des différentes entités juridiques qui le composent.

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

164. 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. Structures complexes et activités inhabituelles ou potentiellement non transparentes

165. Les activités inhabituelles ou potentiellement non transparentes sont des activités qui sont réalisées à travers des entités ou montages juridiques complexes ou dans des territoires qui accusent des déficits en matière de transparence ou qui ne répondent pas aux normes internationales.

166. Les principes directeurs que le conseil d'administration arrête en matière de gouvernance interne prévoient en particulier que les structures complexes et les activités inhabituelles ou potentiellement non transparentes sont soumises à une analyse approfondie et un suivi continu des risques, en particulier ceux liés à la criminalité financière. Qu'il s'agisse d'activités pour compte propre ou pour compte de clients, l'établissement doit comprendre l'utilité de ces structures et maîtriser les risques accompagnant leur création et leur fonctionnement opérationnel.

Sous-chapitre 7.2. Gestion des conflits d'intérêts

167. La politique en matière de gestion des conflits d'intérêts couvre l'ensemble des conflits d'intérêts, pour des raisons économiques, personnelles, professionnelles ou politiques, qu'ils soient persistants ou liés à un événement unique. Une attention particulière doit être portée aux 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 aux membres du conseil d'administration.

168. La politique en matière de gestion des conflits d'intérêts prévoit que tous les conflits d'intérêts actuels et potentiels doivent être détectés, évalués, gérés et atténués ou évités. Lorsque des conflits d'intérêts subsistent, la politique en la matière fixe les procédures à suivre en vue de les rapporter, de les documenter et de les gérer de façon à éviter que l'établissement, ses contreparties et les clients n'en subissent les conséquences injustifiées. La politique et les procédures en question comprennent également la procédure à suivre en cas de non-respect de la politique en question.

169. La politique en matière de gestion des conflits d'intérêts prévoit l'identification des 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 ou son personnel et ses représentants sont ou pourraient être confrontés. Elle prend en considération non seulement les situations et événements du présent pouvant donner lieu à des conflits d'intérêts, mais également le passé récent dans la mesure où les événements en question continuent à avoir un impact potentiel sur l'établissement ou la personne concernée. L'établissement détermine la matérialité des conflits détectés et arrête la manière dont ils doivent être gérés.

170. Afin de minimiser le potentiel de conflits d'intérêts, l'établissement met en place une ségrégation appropriée des tâches et des activités, y compris par le biais d'une gestion des accès à l'information et de dispositifs de type « muraille de Chine » (« Chinese walls »).

171. La politique en matière de gestion des conflits d'intérêts détermine également les procédures de déclaration et d'escalade applicable au sein de l'établissement. 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. 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.[9]

[9] *Cette disposition rejoint celles des articles 441-7 (système moniste) et 442-18 (système dualiste) de la loi du 10 août 1915 concernant les sociétés commerciales, qui disposent que l'administrateur, respectivement le membre du conseil de surveillance ou le membre du directoire qui a un intérêt opposé à celui de la société dans une opération soumise à l'approbation de l'organe concerné, est tenu d'en prévenir l'organe en question et de faire mentionner cette déclaration au procès-verbal de la séance. Il ne peut prendre part à cette délibération.*

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

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

173. Les opérations avec des parties liées sont soumises pour approbation au conseil d'administration lorsqu'elles ont ou pourraient avoir, individuellement ou de manière agrégée, une influence significative et défavorable sur le profil de risque de l'établissement.

174. 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.

175. 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 », transactions aux conditions de marché) ;
- 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 ou sortent des domaines d'activités habituels de l'établissement ;
- sont contraires aux principes d'une gestion saine et prudente dans l'intérêt de l'établissement.

176. 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 (« New Product Approval Process »)

177. La procédure d'approbation des nouveaux produits couvre le développement de nouvelles activités en termes de produits, services, marchés, systèmes et processus ou clientèles ainsi que leurs modifications matérielles et les transactions exceptionnelles.

Elle doit garantir que tout nouveau produit reste cohérent avec les principes directeurs établis par le conseil d'administration, avec la stratégie en matière de risque, l'appétit pour le risque de l'établissement et les limites correspondantes.

178. La procédure d'approbation des nouveaux produits définit en particulier les modifications d'activités sujettes à la procédure d'approbation, les aspects à prendre en considération, les principales questions à examiner ainsi que le déroulement de la procédure d'approbation, y compris les responsabilités de toutes les parties concernées.

Les principales questions à examiner incluent notamment la conformité avec la réglementation, la comptabilité, les modèles tarifaires, l'incidence sur le profil de risque, l'adéquation des fonds propres et la rentabilité, l'allocation de ressources adéquates au front office, au back office et au middle office, ainsi que la disponibilité d'outils internes adéquats et de connaissances techniques suffisantes pour comprendre et contrôler les risques afférents.

179. Ainsi, 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 également l'objet d'une analyse préalable par la fonction compliance.

180. 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 précédent soient disponibles.

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

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

182. 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.

183. Lorsqu'une sous-traitance ou une chaîne de sous-traitances est exclusivement de nature informatique et qu'au moins une des sous-traitances correspond à la définition du *cloud computing* de la circulaire CSSF 17/654, les exigences du présent sous-chapitre ne s'appliquent pas et il convient à l'établissement de respecter les exigences de la circulaire CSSF 17/654.

L'exception décrite au paragraphe précédent ne s'applique pas aux sous-traitances de nature métier ou administrative (« business process outsourcing ») qui reposent sur une infrastructure de *cloud computing* sous-traitée.

Section 7.4.1. Exigences générales en matière de sous-traitance

184. La sous-traitance ne doit pas aboutir à ce que les règles de la présente circulaire en matière d'administration centrale 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 ;
- L'établissement veille à la protection des données concernées par une sous-traitance, conformément au règlement général sur la protection des données (RGPD) et aux exigences de l'autorité compétente en la matière, la Commission nationale pour la protection des données (CNPD) ;
- En cas de sous-traitance, l'établissement applique les dispositions de l'article 41, paragraphe 2bis de la LSF en matière de secret professionnel ;
- 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 ;
- La responsabilité finale de la gestion des risques associés à la sous-traitance incombe à l'établissement procédant à la sous-traitance ;

- La confidentialité et l'intégrité des données et des systèmes doivent être maîtrisées dans toute la chaîne de sous-traitance. Notamment, l'accès aux données et systèmes doit respecter les principes du « besoin de savoir » et du « moindre privilège » : l'accès n'est octroyé qu'aux personnes dont la fonction le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions ;
- L'établissement qui a l'intention de sous-traiter une activité matérielle doit obtenir l'autorisation préalable de la CSSF. Une notification à la CSSF, justifiant que les conditions fixées dans la présente circulaire sont respectées, est suffisante lorsque l'établissement recourt à un établissement de crédit luxembourgeois ou à un PSF de support selon les articles 29-1 à 29-6 de la LSF ;
- L'accès de la CSSF, du réviseur d'entreprises agréé et des fonctions de contrôle interne de l'établissement aux informations relatives aux activités sous-traitées doit être garanti en vue de leur permettre d'émettre une opinion fondée sur l'adéquation de la sous-traitance. Cet accès inclut que les précités peuvent également vérifier les données pertinentes détenues par un partenaire externe et, dans les cas prévus par la législation nationale applicable, 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.

185. 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. L'analyse comprendra une évaluation détaillée (due diligence) du prestataire de services proposé.

186. 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.

187. 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.

188. 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.

189. 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 et notamment les risques opérationnels qui en découlent, comme le risque juridique, le risque informatique, le risque de réputation ou encore le risque de concentration (au niveau du prestataire de services). Elle fixe les exigences applicables en matière de sous-traitance, de la phase préparatoire jusqu'à l'expiration ou la résiliation en passant par le reporting, auxquelles sont soumis les prestataires et détermine 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'en entraver la surveillance par la CSSF.

190. Une attention particulière doit être accordée aux aspects de continuité et au caractère révocable de la sous-traitance. L'établissement doit être capable de maintenir ses fonctions critiques en cas d'évènements exceptionnels ou de crises. A ce titre, les contrats de sous-traitance prévoient un préavis de résiliation d'une durée suffisante pour permettre à l'établissement de prendre les mesures nécessaires afin de garantir la continuité des services sous-traités et ne contiennent pas de clause de résiliation ou d'arrêt des prestations en raison de l'application à l'établissement de mesures de résolution ou d'assainissement ou d'une procédure de liquidation telles que prévues dans la loi du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement. 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 prestataire ou de les reprendre en gestion propre, chaque fois que la continuité ou la qualité de la prestation de service risque d'être compromise.

191. Pour chaque activité sous-traitée, l'établissement désignera parmi son personnel 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

192. L'établissement met en place une politique informatique qui couvre l'ensemble des activités informatiques réparties entre l'établissement et tous les intervenants de la chaîne de sous-traitance. 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. L'établissement prévoit également un contrôle régulier des sauvegardes et des capacités à restaurer ces sauvegardes.

193. 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.

194. 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

195. 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. Au cas où ces systèmes contiennent des données confidentielles lisibles concernant les clients, l'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.
- A l'étranger, auprès :
  - de tout prestataire informatique, y compris auprès d'une entité du groupe auquel l'établissement appartient. Au cas où ces systèmes contiennent des données confidentielles lisibles concernant les clients, l'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.

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

196. 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.

197. Des tiers sous-traitants qui fournissent des services de conseil, de développement ou de maintenance doivent intervenir par défaut hors du système informatique de production. Un accord exprès de l'établissement est nécessaire pour chacune des interventions sur le système 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 et que les dispositions de l'article 41, paragraphe 2bis de la LSF soient respectées.

198. 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.

199. 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

200. L'infrastructure informatique peut appartenir à l'établissement ou être mise à disposition par le sous-traitant.

Lorsque l'infrastructure informatique contient des données confidentielles lisibles concernant les clients, l'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF. A défaut, le sous-traitant 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.

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 d'opérateur.

201. 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.

202. 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 ce prestataire n'agisse pas en tant qu'opérateur. Si le prestataire a un accès physique ou logique sur les systèmes de l'établissement, l'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.

203. 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 sans être protégée. La confidentialité et l'intégrité des données et des systèmes doivent être maîtrisées dans toute la chaîne de sous-traitance. Notamment, l'accès aux données et systèmes doit respecter les principes du « besoin de savoir » et du « moindre privilège » : l'accès n'est octroyé qu'aux personnes dont la fonction le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions. L'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.

Section 7.4.3. Exigences générales supplémentaires

204. 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 les membres de son personnel 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.

205. 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).

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

207. 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.

Section 7.4.4. Documentation

208. 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. Cette politique en matière de sous-traitance est actualisée et ré-approuvée à intervalles réguliers par le conseil d'administration, pour que les modifications appropriées soient rapidement mises en œuvre par la direction autorisée. Tout accord de sous-traitance fait l'objet d'un contrat officiel et détaillé (cahier des charges inclus).

209. 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.

210. 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

211. Pour les entreprises d'investissement, les rapports ICAAP/ILAAP et l'attestation annuelle de conformité avec les exigences de la présente circulaire émis par la direction autorisée ainsi que les rapports de synthèse des fonctions de contrôle interne sont communiqués à la CSSF. Ces informations sont à soumettre à la CSSF au plus tard un mois après la tenue de l'assemblée générale ordinaire de l'établissement 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. Le cadre de gestion des risques à l'échelle de l'établissement

Section 1.1.1. Généralités

1. Les établissements mettent en place un cadre de gestion des risques cohérent et exhaustif, à l'échelle de l'établissement, couvrant l'ensemble des activités et des unités opérationnelles de l'établissement, y compris les fonctions de contrôle interne, et reconnaissant pleinement la substance économique de toutes leurs expositions au risque, permettant à l'organe de direction de garder sous maîtrise l'ensemble des risques auxquels l'établissement est ou pourrait être exposé.

2. Le cadre de gestion des risques doit comprendre un ensemble de politiques et de procédures, de limites, de contrôles et d'alertes qui permettent d'identifier, de mesurer, de gérer ou d'atténuer et de déclarer ces risques au niveau des unités opérationnelles, de l'établissement dans son ensemble, comprenant, s'il y a lieu, les niveaux consolidés et sous-consolidés.

Section 1.1.2. Politiques spécifiques (de risque, de fonds propres et de liquidités)

3. La politique de risque, qui met en œuvre la stratégie définie par le conseil d'administration en matière de risques, comprend :
   - la détermination de l'appétit au risque de l'établissement ;

- 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 l'appétit au risque défini par l'établissement. 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 ;
- 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, de seuils d'alerte 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).

La politique de risque explique comment les différents risques sont identifiés, mesurés, gérés, contrôlés et déclarés. 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.

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

4. 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.

Section 1.1.3. Détection, gestion, mesure et déclaration des risques

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

6. 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 risques et de fonds propres et de réserves de liquidité.

7. La gestion des risques envers des parties liées est intégrée dans tous les éléments du dispositif de gouvernance interne.

8. 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.

9. 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.

10. 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), basés sur des analyses structurées et documentées.

Chapitre 2. Risques de concentration

11. Les risques de concentration résultent notamment d'expositions importantes concentrées sur des clients, des contreparties ou des fournisseurs de services respectivement des groupes de clients, contreparties ou fournisseurs de services liés, y compris des parties liées, sur des pays ou des secteurs (industries) ou encore sur des produits ou des marchés spécifiques (concentration intra-risques). Ces expositions ne se limitent 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 - notamment ceux liés à la sous-traitance - 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.

    Le risque de concentration doit faire l'objet d'une vigilance particulière et d'un effort d'identification car il est de nature à mettre en péril la stabilité financière de l'établissement.

Chapitre 3. Tarification du risque (« Risk Transfer Pricing »)

12. Les établissements mettent en 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 l'appétit au risque et au principe d'une gestion saine et prudente des affaires.

13. 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 membres concernés du personnel. La comparabilité et la cohérence des systèmes des prix de cession interne utilisées au sein du groupe doit être assurée.

14. 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 4. Gestion de fortune et activités associées (activités de « private banking »)

15. La gestion de fortune (« wealth management ») et ses activités associées sont particulièrement exposées aux risques de blanchiment de capitaux ou de financement du terrorisme. En conséquence, les établissements prestant ces activités porteront une attention particulière au respect des obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, qu'elles soient de nature réglementaire, qu'elles découlent de politiques et procédures internes ou qu'elles relèvent du domaine des bonnes pratiques et des recommandations d'organisations faisant autorité dans ce domaine.

16. Ces établissements disposent de processus solides pour garantir que les relations d'affaires avec leurs clients soient 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.

17. Ces 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.

18. Ces 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.

19. Les entrées et sorties physiques d'espèces, de titres ou d'autres objets de valeur doivent être effectués ou contrôlés par une fonction séparée de la fonction commerciale.

20. L'encodage et la modification des données signalétiques des clients doivent être effectués ou contrôlés par une fonction indépendante de la fonction commerciale.

21. 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.

22. Ces établissements doivent disposer d'un processus solide d'encadrement de crédits (ou prêts) octroyés dans le cadre de la prestation du service auxiliaire visé au point 2. de la Section C de l'annexe II de la LSF. 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. Ces établissements doivent disposer d'un « early warning system » indépendant de la fonction commerciale qui organise la surveillance de la valeur des garanties financières et déclenche le processus de liquidation des garanties financières. Il doit être assuré que le processus de liquidation soit déclenché suffisamment à temps et en tout cas avant que la valeur des garanties ne devienne inférieure au crédit. Les contrats avec les clients doivent décrire clairement la procédure déclenchée en cas d'insuffisance des garanties.

Chapitre 5. Risques liés aux entités shadow banking

23. Ce chapitre s'applique uniquement aux établissements auxquels s'applique la quatrième partie (grands risques) du règlement CRR, conformément au niveau d'application prévu à la première partie, titre II, dudit règlement.

Sous-chapitre 5.1. Mise en œuvre de principes de contrôle interne solides

24. Ces établissements mettent en place un cadre interne dédié permettant de recenser, de gérer, de contrôler et d'atténuer les risques liés aux expositions sur les entités dites « entités du système bancaire parallèle » (« entités shadow banking »[10]) conformément aux EBA/GL/2015/20.

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

25. Ces établissements appliquent un seuil de matérialité dédié pour identifier les expositions sur des entités shadow banking. Conformément aux EBA/GL/2015/20, toute exposition individuelle sur une entité shadow banking qui est supérieure ou égale à 0,25%[11] des fonds propres éligibles de l'établissement[12], après prise en compte des effets d'atténuation du risque de crédit et des exemptions[13], doit être prise en considération et ne peut pas être considérée comme une exposition de « faible importance ».

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

Sous-chapitre 5.2. Application de limites quantitatives

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

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

29. Dans sa fixation d'une limite agrégée pour les expositions sur des entités shadow banking, chacun de ces établissements doit tenir compte de :
    - son modèle d'entreprise, de son cadre de gestion du risque et de son profil d'appétence au risque ;
    - la taille de ses expositions actuelles sur des entités shadow banking par rapport à ses expositions totales et par rapport à ses expositions totales sur des entités réglementées du secteur financier ;
    - l'interconnexion entre entités shadow banking, d'une part, et entre les entités shadow banking et l'établissement, d'autre part.

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

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

[12] *Au sens de l'article 4, paragraphe 1, point 71, du règlement CRR.*

[13] *i) Effets d'atténuation du risque de crédit conformément aux articles 399 et 403 du règlement CRR,*

ii) Exemptions prévues aux articles 400 et 493, paragraphe 3 du règlement CRR.

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

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

33. L'approche de repli doit être appliquée comme suit :
    - Si certains établissements ne peuvent satisfaire aux exigences concernant les processus et les mécanismes de contrôle efficaces ou la supervision par leur organe de direction, telles que prévues au chapitre 4 des EBA/GL/2015/20, ils doivent appliquer l'approche de repli à la totalité de leurs expositions sur des entités shadow banking (à savoir, la somme de leurs expositions sur des entités shadow banking).

- Si certains établissements peuvent satisfaire aux exigences concernant les processus et les mécanismes de contrôle efficaces ou la supervision par leur organe de direction, telles que prévues au sous-chapitre 5.1 de cette partie, mais ne peuvent réunir suffisamment d'informations pour leur permettre de fixer des limites appropriées, comme prévu au sous-chapitre 5.2, ils ne doivent appliquer l'approche de repli qu'aux expositions sur des entités shadow banking pour lesquelles les établissements ne peuvent réunir suffisamment d'informations. L'approche de base telle que décrite au sous-chapitre 5.2 doit être appliquée aux expositions restantes sur des entités shadow banking.

Chapitre 6. Risque de taux d'intérêt

Sous-chapitre 6.1. Risque de taux d'intérêt inhérent aux activités autres que de négociation

34. Dans leur mise en œuvre de l'article 14 (Risque de taux d'intérêt inhérent aux activités hors portefeuille de négociation) du RCSSF 15-02, les entreprises d'investissement CRR se conforment aux orientations de l'EBA sur la gestion du risque de taux d'intérêt inhérent aux activités hors portefeuille de négociation (Guidelines on the management of interest rate risk arising from non-trading book activities « EBA /GL/2018/02 »).

Sous-chapitre 6.2. Corrections de la duration modifiée des titres de créance

35. Les entreprises d'investissement CRR qui appliquent l'approche standard pour le calcul de leurs exigences de fonds propres liées au risque de taux d'intérêt général sont tenus d'appliquer des modifications au calcul de la duration pour tenir compte du risque de remboursement anticipé des titres de créance. Les entreprises d'investissement CRR appliquent l'une des deux méthodes de correction de la duration modifiée prévues par les orientations de l'EBA sur les corrections de la duration modifiée des titres de créance en vertu de l'article 340, paragraphe 3, deuxième alinéa, du règlement CRR (Guidelines on corrections to modified duration for debt instruments under the second subparagraph of Article 340(3) of Regulation (EU) 575/2013 « EBA/GL/2016/09 »).

Chapitre 7. Risques liés à la conservation d'actifs financiers par des tiers

36. Les établissements se dotent d'une politique en matière de sélection des dépositaires auprès desquels ils conservent les actifs financiers appartenant à leurs clients. Cette politique établit des critères minimaux de qualité auxquels un dépositaire doit répondre.
37. Les établissements effectuent un contrôle diligent (due diligence) préalable à la conclusion d'un contrat avec un dépositaire et exercent une surveillance continue sur le dépositaire pendant toute la durée de la relation, afin de s'assurer que ces critères de qualité restent respectés.
38. Les établissements procèdent à des réconciliations régulières entre les avoirs enregistrés dans leur comptabilité comme appartenant aux clients et ceux confirmés par leurs dépositaires.

Partie IV. Entrée en vigueur

La présente circulaire abroge et remplace la circulaire CSSF 12/552, telle que modifiée par les circulaires CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655 et 20/750, dans le chef des entreprises d'investissement et est applicable à partir du 1er janvier 2021.

Les lignes directrices, orientations et recommandations citées dans la présente circulaire peuvent être consultées et téléchargées sur les sites internet respectifs de l'EBA (www.eba.europa.eu), de l'ESMA (www.esma.europa.eu) et du BCBS (https://www.bis.org/bcbs/index.htm).

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annexe : Extraits de la section 9.3 des EBA/GL/2017/12, membres indépendants de l'organe de direction dans sa fonction de surveillance d'un établissement CRD

Annexe I - Extraits de la section 9.3 des EBA/GL/2017/12, membres indépendants de l'organe de direction dans sa fonction de surveillance d'un établissement CRD

91. Sans préjudice du point 92, dans les situations suivantes il est présumé qu'un membre de l'organe de direction dans sa fonction de surveillance d'un établissement CRD est considéré comme «n'étant pas indépendant»:

a. le membre détient ou a détenu un mandat de membre de l'organe de direction dans sa fonction exécutive au sein d'un établissement entrant dans le périmètre de consolidation prudentielle, sauf s'il n'a pas occupé un tel poste au cours des 5 dernières années;

b. le membre est un actionnaire qui contrôle l'établissement CRD, déterminé par référence aux cas énoncés à l'article 22, paragraphe 1, de la directive 2013/34/UE, ou représente les intérêts d'un actionnaire qui le contrôle, y compris lorsque le propriétaire est un État membre ou un autre organisme public;

c. le membre a une relation financière ou commerciale significative avec l'établissement CRD;

d. le membre est un employé d'un actionnaire qui contrôle l'établissement CRD ou est associé de quelque manière que ce soit avec un actionnaire qui contrôle l'établissement CRD;

e. le membre est employé par quelqu'entité que ce soit entrant dans le périmètre de consolidation, sauf lorsque les deux conditions suivantes sont cumulativement réunies:

i. le membre n'appartient pas au niveau hiérarchique le plus élevé de l'établissement, qui rend directement compte à l'organe de direction;

ii. le membre a été élu à la fonction de surveillance dans le cadre d'un système de représentation des employés et la législation nationale prévoit une protection adéquate contre le licenciement abusif et les autres formes de traitement inéquitable;

f. le membre a été employé auparavant à un poste au plus haut niveau hiérarchique dans l'établissement CRD ou dans une autre entité entrant dans son périmètre de consolidation prudentielle, rendant directement de compte uniquement à l'organe de direction, et la période écoulée entre la fin de cet emploi et le mandat au sein de l'organe de direction est inférieure à 3 ans;

g. le membre a été, au cours d'une période de 3 ans, le mandant d'un conseiller professionnel significatif, un auditeur externe ou un conseiller significatif de l'établissement CRD ou d'une autre entité entrant dans son périmètre de consolidation prudentielle ou un employé associé de manière significative au service fourni;

h. le membre est ou a été, au cours de l'année écoulée, un fournisseur significatif ou un client significatif de l'établissement CRD ou d'une autre entité entrant dans son périmètre de consolidation prudentielle ou avait une autre relation commerciale significative ou est un cadre supérieur d'un fournisseur significatif, d'un client ou d'une entité commerciale ayant une relation commerciale significative ou est directement ou indirectement associé à un fournisseur significatif, un client ou une entité commerciale ayant une relation commerciale significative;

i. le membre reçoit, outre la rémunération pour son rôle et la rémunération dans le cadre de son emploi conformément au point e), des honoraires ou autres prestations significatifs de la part de l'établissement CRD ou d'une autre entité entrant dans son périmètre de consolidation prudentielle;

j. le membre a été membre de l'organe de direction de l'entité pendant 12 années consécutives ou plus;

k. le membre est un membre de la famille proche d'un membre de l'organe de direction dans sa fonction exécutive de l'établissement CRD ou d'une autre entité entrant dans son périmètre de consolidation prudentielle ou une personne dans une situation visée aux points a) à h).

92. Le simple fait de relever d'une ou de plusieurs des situations visées au point 91 ne permet pas automatiquement de qualifier un membre de non indépendant. Lorsqu'un membre relève d'une ou de plusieurs des situations énoncées au point 91, l'établissement CRD peut démontrer à l'autorité compétente que le membre devrait néanmoins être considéré comme indépendant. À cette fin, les établissements CRD devraient être en mesure de justifier à l'autorité compétente les raisons pour lesquelles la capacité du membre d'exercer un jugement objectif et équilibré et de prendre des décisions de manière indépendante n'est pas affectée par la situation.

93. Aux fins du point 92, les établissements CRD devraient considérer que le fait d'être actionnaire, titulaire de comptes privés ou emprunteur ou utilisateur d'autres services d'un établissement CRD, sauf dans les cas explicitement énumérés dans cette section, ne devrait pas mener à une situation où le membre est considéré comme non indépendant, dès lors qu'il demeure en-deçà d'un seuil de minimis approprié. De telles relations devraient être prises en compte dans le cadre de la gestion des conflits d'intérêts conformément aux orientations de l'ABE sur la gouvernance interne.

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu