



Commission de Surveillance  
du Secteur Financier

# Circulaire CSSF 20/759

MISE À JOUR DE 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, CSSF  
20/750 ET CSSF 20/759,  
RELATIVE À  
L'ADMINISTRATION CENTRALE,  
LA GOUVERNANCE INTERNE ET  
LA GESTION DES RISQUES

## Circulaire 20/759

**Concerne:** Mise à jour de 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, CSSF 20/750 et CSSF 20/758, relative à l'administration centrale, la gouvernance interne et la gestion des risques.

Luxembourg, le 7 décembre 2020

Mesdames, Messieurs,

**À tous les établissements de  
crédit et professionnels  
effectuant des opérations de  
prêt**

1. Par la présente circulaire, la CSSF, en sa qualité d'autorité compétente, se conforme aux orientations de l'Autorité Bancaire Européenne répertoriées au point 2. La CSSF intègre ces orientations dans sa pratique administrative et son approche réglementaire en vue de promouvoir la convergence des pratiques de surveillance dans ce domaine au niveau européen.
2. Sont visées les orientations suivantes :
  - (1) de gouvernance interne (Guidelines on internal governance « EBA/GL/2017/11 ») et
  - (2) des orientations communes de l'EBA et de l'Autorité européenne des marchés financiers (« ESMA ») en matière d'éligibilité des membres d'organes de direction (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 ») ;
  - (3) d'application de la définition du défaut au titre de l'article 178 du règlement (UE) n° 575/2013 (Guidelines on the application of the definition of default under Article 178 of Regulation (EU) No 575/2013 « EBA/GL/2016/07 »),
  - (4) de spécification des types d'expositions devant être considérés comme présentant un risque élevé (Guidelines on specification of types of exposures to be associated with high risk « EBA/GL/2019/01 »),
  - (5) de 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 »),
  - (6) de corrections de la durée modifiée des titres de créance en vertu de l'article 340, paragraphe 3, deuxième alinéa, du règlement (UE) n° 575/2013 (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 »).

3. Les orientations susmentionnées ont été incorporées dans la circulaire CSSF 12/552 sur l'administration centrale, la gouvernance interne et la gestion des risques. En même temps, la terminologie et les définitions de la circulaire ont été revues et certaines dispositions ont été précisées. Une version de la circulaire permettant de retracer les changements opérés se trouve en annexe.
4. Les principaux changements concernent :
  - a. L'extension du champ d'application aux compagnies financières holding et compagnies financières holding mixte ;
  - b. Une articulation plus précise du concept de proportionnalité, par son rattachement à la notion d'établissement systémique au sens de la loi du 5 avril 1993 sur le secteur financier ;
  - c. Des précisions sur l'application de la proportionnalité dans la mise en place de fonctions de contrôle interne ;
  - d. Le renforcement de l'organe de direction dans sa fonction de surveillance à travers des dispositions renforcées en matière de diversité et d'indépendance ;
  - e. La prise en compte des facteurs de risque environnementaux, sociétaux et de gouvernance (ESG) en vue d'assurer la viabilité du modèle d'affaires ;
  - f. L'introduction d'un chapitre sommaire dédié aux risques découlant de l'activité de banque dépositaire.
5. La circulaire CSSF 12/552, telle que remaniée, est applicable dans son intégralité aux établissements de crédit et en partie aux professionnels effectuant des opérations de prêt. Une circulaire séparée couvre dorénavant les entreprises d'investissement.
6. La présente circulaire est applicable à partir du 1<sup>er</sup> janvier 2021.

**Claude WAMPACH**  
Directeur

**Marco ZWICK**  
Directeur

**Jean-Pierre FABER**  
Directeur

**Françoise KAUTHEN**  
Directeur

**Claude MARX**  
Directeur général

Annexe

- o Rouge pour les ajouts/suppressions
- o Vert pour les déplacements de texte

## 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, CSSF 20/750 et CSSF 20/759

Concerne : Administration centrale, gouvernance interne et gestion des risques

Luxembourg, le ~~11 décembre~~  
~~2012~~ 27 décembre 2020

A tous les établissements de  
crédit, ~~entreprises~~  
~~d'investissement~~ et  
professionnels effectuant des  
opérations de prêt<sup>1</sup>

Mesdames, Messieurs,

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

<sup>1</sup> Pour les professionnels effectuant des opérations de prêt, tels que définis à l'article 28-4 de la loi du 5 avril 1993 relative au secteur financier, le chapitre 3 de la partie III est applicable à l'exception du sous-chapitre 3.4 « Expositions présentant un risque particulièrement élevé ». Le paragraphe 12 du chapitre 2 de la partie III est également applicable.

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

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

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

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

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

<sup>2</sup> Circulaires IML 96/126 concernant l'organisation administrative et comptable, IML 98/143 concernant le contrôle interne, CSSF 04/155 concernant la fonction compliance, CSSF 05/178 concernant l'organisation administrative et comptable et la sous-traitance en matière informatique et CSSF 10/466 concernant les informations à publier en situations de crise.

<sup>3</sup> Les circulaires IML 95/120, IML 96/126, IML 98/143 restent en vigueur pour les PSF qui ne sont pas des entreprises d'investissement ainsi que la circulaire CSSF 11/656 qui abroge et remplace la CSSF 05/178. Ces circulaires, ensemble avec la circulaire CSSF 04/155, restent d'application pour les établissements de paiement et les établissements de monnaie électronique.

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

Pour ce qui concerne les établissements CRR, La présente circulaire précise les mesures que doivent prendre les établissements de crédit en exécution des dispositions de la LSF et du RCSSF 15-02 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 bancaire 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 de crédit se reportent aux principes énoncés à la partie I, chapitre 2 ainsi qu'aux orientations et recommandations listées en partie IV de la présente circulaire 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'organes de direction (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 »).

Les principes et bonnes pratiques découlant d'autres sources déjà repris dans les versions précédentes de la circulaire sont maintenus dans la mesure où ceux-ci ne sont pas devenus obsolètes.

S'agissant de nominations de membres de l'organe de direction et de titulaires de fonctions clés, la présente circulaire doit se lire en parallèle avec le règlement CSSF N° 15-02 relatif au processus de contrôle et d'évaluation prudentiels s'appliquant aux établissements GRR, la Procédure prudentielle en la matière publiée sur le site internet de la CSSF.

Les multiples circulaires existantes relatives aux risques et à leur gestion seront rassemblées au sein d'une version ultérieure de la présente circulaire. Lorsqu'en réponse à des développements réglementaires sur le plan international ou des nécessités locales, la CSSF est amenée à préciser les exigences reprises dans la présente circulaire, elle procédera à la mise à jour de cette circulaire. La partie IV de la circulaire contient une chronologie des mises à jour qui permet au lecteur de retracer les modifications opérées par les mises à jour successives.

La circulaire est divisée en quatre parties : la première partie contient 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 et les mesures transitoires et dispositions abrogatoires. La table des matières se présente comme suit, la chronologie des mises à jour permettant au lecteur de retracer les modifications opérées par les mises à jour successives.

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

## TABLE DES MATIÈRES

<u>Partie I. Définitions et champ d'application</u>	<u>14</u>
<u>Chapitre 1. Définitions et abréviations</u>	<u>14</u>
<u>Chapitre 2. Champ d'application et proportionnalité</u>	<u>17</u>
<u>Partie II. Dispositif en matière d'administration centrale et de gouvernance interne</u>	<u>20</u>
<u>Chapitre 1. L'administration centrale</u>	<u>20</u>
<u>Chapitre 2. Le dispositif de gouvernance interne</u>	<u>21</u>

<u>Chapitre 3. Propriétés génériques d'un dispositif « solide » en matière d'administration centrale et de gouvernance interne</u>	23
<u>Chapitre 4. Organe de surveillance et direction autorisée</u>	25
<u>Sous-chapitre 4.1. L'organe de surveillance</u>	25
<u>Section 4.1.1. Responsabilités de l'organe de surveillance</u>	25
<u>Section 4.1.2. Composition et qualification de l'organe de surveillance</u>	29
<u>Section 4.1.3. Organisation et fonctionnement de l'organe de surveillance</u>	31
<u>Section 4.1.4. Comités spécialisés</u>	33
<u>Sous-section 4.1.4.1. Le comité d'audit</u>	35
<u>Sous-section 4.1.4.2. Le comité des risques</u>	37
<u>Sous-chapitre 4.2. La direction autorisée</u>	39
<u>Section 4.2.1. Responsabilités de la direction autorisée</u>	39
<u>Section 4.2.2. Qualification de la direction autorisée</u>	43
<u>Chapitre 5. Organisation administrative, comptable et informatique</u>	44
<u>Sous-chapitre 5.1. L'organigramme et les ressources humaines</u>	44
<u>Sous-chapitre 5.2. Les procédures et la documentation interne</u>	46
<u>Sous-chapitre 5.3. L'infrastructure administrative et technique</u>	47
<u>Section 5.3.1. L'infrastructure administrative des fonctions commerciales</u>	47
<u>Section 5.3.2. La fonction financière et comptable</u>	47
<u>Section 5.3.3. La fonction informatique</u>	49
<u>Section 5.3.4. Le dispositif de communication et d'alerte interne et externe</u>	50
<u>Section 5.3.5. Le dispositif de gestion de crises</u>	50
<u>Chapitre 6. Le contrôle interne</u>	52
<u>Sous-chapitre 6.1. Les contrôles opérationnels</u>	53
<u>Section 6.1.1. Contrôles quotidiens réalisés par le personnel exécutant</u>	53
<u>Section 6.1.2. Contrôles critiques continus</u>	54
<u>Section 6.1.3. Contrôles réalisés par les membres de la direction autorisée sur les activités ou fonctions qui tombent sous leur responsabilité directe</u>	54
<u>Sous-chapitre 6.2. Les fonctions de contrôle interne</u>	55
<u>Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne</u>	56
<u>Section 6.2.2. Caractéristiques des fonctions de contrôle interne</u>	56
<u>Section 6.2.3. Exécution des travaux des fonctions de contrôle interne</u>	58
<u>Section 6.2.4. Organisation des fonctions de contrôle interne</u>	60
<u>Section 6.2.5. La fonction de contrôle des risques</u>	63

<u>Sous-section 6.2.5.1. Responsabilités spécifiques et champ d'application de la fonction de contrôle des risques</u>	<u>65</u>
<u>Sous-section 6.2.5.2. Organisation de la fonction de contrôle des risques</u>	<u>67</u>
<u>Section 6.2.6. La fonction compliance</u>	<u>68</u>
<u>Sous-section 6.2.6.1. La charte de compliance</u>	<u>69</u>
<u>Sous-section 6.2.6.2. Champ d'application et responsabilités spécifiques de la fonction compliance</u>	<u>70</u>
<u>Sous-section 6.2.6.3. Organisation de la fonction compliance</u>	<u>73</u>
<u>Section 6.2.7. La fonction d'audit interne</u>	<u>73</u>
<u>Sous-section 6.2.7.1. La charte d'audit interne</u>	<u>74</u>
<u>Sous-section 6.2.7.2. Responsabilités spécifiques et champ d'application de la fonction d'audit interne</u>	<u>76</u>
<u>Sous-section 6.2.7.3. Exécution des travaux d'audit interne</u>	<u>77</u>
<u>Sous-section 6.2.7.4. Organisation de la fonction d'audit interne</u>	<u>79</u>
<u>Chapitre 7. Exigences spécifiques</u>	<u>80</u>
<u>Sous-chapitre 7.1. Structure organisationnelle et entités juridiques (« Know-your-structure »)</u>	<u>80</u>
<u>Section 7.1.1. Structures complexes et activités inhabituelles ou potentiellement non transparentes</u>	<u>81</u>
<u>Sous-chapitre 7.2. Gestion des conflits d'intérêts</u>	<u>81</u>
<u>Section 7.2.1. Exigences spécifiques relatives aux conflits d'intérêts en relation avec des parties liées</u>	<u>83</u>
<u>Sous-chapitre 7.3. Procédure d'approbation des nouveaux produits (« New Product Approval Process »)</u>	<u>84</u>
<u>Sous-chapitre 7.4. Sous-traitance (« Outsourcing »)</u>	<u>85</u>
<u>Section 7.4.1. Exigences générales en matière de sous-traitance</u>	<u>86</u>
<u>Section 7.4.2. Exigences particulières en matière de sous-traitance dans le domaine informatique</u>	<u>89</u>
<u>Sous-section 7.4.2.1. Services de gestion/d'opération des systèmes informatiques</u>	<u>89</u>
<u>Sous-section 7.4.2.2. Services de conseil, de développement et de maintenance</u>	<u>90</u>
<u>Sous-section 7.4.2.3. Services d'hébergement et propriété de l'infrastructure</u>	<u>91</u>
<u>Section 7.4.3. Exigences générales supplémentaires</u>	<u>92</u>
<u>Section 7.4.4. Documentation</u>	<u>93</u>
<u>Chapitre 8. Reporting légal</u>	<u>94</u>
<u>Partie III. Gestion des risques</u>	<u>94</u>

<u>Chapitre 1. Principes généraux en matière de mesure et de gestion des risques</u>	94
<u>Sous-chapitre 1.1. Le cadre de gestion des risques à l'échelle de l'établissement</u>	94
<u>Section 1.1.1. Généralités</u>	94
<u>Section 1.1.2. Politiques spécifiques (de risque, de fonds propres et de liquidités)</u>	94
<u>Section 1.1.3. Détection, gestion, mesure et déclaration des risques</u>	96
<u>Chapitre 2. Risques de concentration</u>	97
<u>Chapitre 3. Risque de crédit</u>	98
<u>Sous-chapitre 3.1. Principes généraux</u>	98
<u>Sous-chapitre 3.2. Crédits immobiliers résidentiels aux particuliers</u>	100
<u>Sous-chapitre 3.3. Crédits aux promoteurs immobiliers</u>	101
<u>Sous-chapitre 3.4. Expositions présentant un risque particulièrement élevé</u>	102
<u>Sous-chapitre 3.5. Expositions non performantes et expositions restructurées</u>	102
<u>Chapitre 4. Tarification du risque (« Risk Transfer Pricing »)</u>	103
<u>Chapitre 5. Gestion patrimoniale privée (« banque privée »)</u>	104
<u>Chapitre 6. Risques liés aux entités shadow banking</u>	105
<u>Sous-chapitre 6.1. Mise en œuvre de principes de contrôle interne solides</u>	105
<u>Sous-chapitre 6.2. Application de limites quantitatives</u>	106
<u>Chapitre 7. Risque de charge pesant sur les actifs (« asset encumbrance »)</u>	108
<u>Chapitre 8. Risque de taux d'intérêt</u>	109
<u>Sous-chapitre 8.1. Risque de taux d'intérêt inhérent aux activités autres que de négociation</u>	109
<u>Sous-chapitre 8.2. Corrections de la durée modifiée des titres de créance</u>	109
<u>Chapitre 9. Risques liés à la conservation d'actifs financiers par des tiers</u>	110
<u>Partie IV. Chronologie</u>	110
<u>Partie I. Définitions et champ d'application</u>	10
<u>Chapitre 1. Définitions</u>	10
<u>Chapitre 2. Champ d'application</u>	10
<u>Partie II. Dispositif en matière d'administration centrale et de gouvernance interne</u>	12
<u>Chapitre 1. L'administration centrale</u>	12
<u>Chapitre 2. Le dispositif de gouvernance interne</u>	13
<u>Chapitre 3. Propriétés génériques d'un dispositif « solide » en matière d'administration centrale et de gouvernance interne</u>	15
<u>Chapitre 4. Conseil d'administration et direction autorisée</u>	17
<u>Sous-chapitre 4.1. Le conseil d'administration</u>	17

Section 4.1.1. — Responsabilités du conseil d'administration	17
Section 4.1.2. — Composition et qualification du conseil d'administration	21
Section 4.1.3. — Organisation et fonctionnement du conseil d'administration	22
Section 4.1.4. — Comités spécialisés	23
Sous-section 4.1.4.1. — Le comité d'audit	24
Sous-section 4.1.4.2. — Le comité des risques	25
Sous-chapitre 4.2. — La direction autorisée	26
Section 4.2.1. — Responsabilités de la direction autorisée	26
Section 4.2.2. — Qualification de la direction autorisée	30
Section 4.2.3. — Politiques spécifiques (de risque, de fonds propres et de liquidités)	30
Chapitre 5. — Organisation administrative, comptable et informatique	31
Sous-chapitre 5.1. — L'organigramme et les ressources humaines	31
Sous-chapitre 5.2. — L'infrastructure administrative et technique	32
Section 5.2.1. — L'infrastructure administrative des fonctions commerciales	32
Section 5.2.2. — La fonction financière et comptable	33
Section 5.2.3. — La fonction informatique	35
Section 5.2.4. — Le dispositif de communication et d'alerte internes	35
Section 5.2.5. — Le dispositif de gestion de crises	36
Sous-chapitre 5.3. — La documentation interne	36
Chapitre 6. — Le contrôle interne	37
Sous-chapitre 6.1. — Les contrôles opérationnels	38
Section 6.1.1. — Contrôles quotidiens réalisés par le personnel exécutant	38
Section 6.1.2. — Contrôles critiques continus	38
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	39
Section 6.2.1. — Responsabilités génériques des fonctions de contrôle interne	40
Section 6.2.2. — Caractéristiques des fonctions de contrôle interne	41
Section 6.2.3. — Exécution des travaux des fonctions de contrôle interne	42
Section 6.2.4. — Organisation des fonctions de contrôle interne	43
Section 6.2.5. — La fonction de contrôle des risques	45
Sous-section 6.2.5.1. — Responsabilités spécifiques et champ d'application 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	47
Sous-section 6.2.6.1.	La charte de compliance	48
Sous-section 6.2.6.2.	Responsabilités spécifiques et champ d'application de la fonction compliance	49
Sous-section 6.2.6.3.	Organisation de la fonction compliance	51
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	53
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	56
Chapitre 7.	Exigences spécifiques	57
Sous-chapitre 7.1.	Structure organisationnelle et entités juridiques (« Know-your-structure »)	57
Section 7.1.1.	Principes directeurs en matière d'activités « inhabituelles » ou « non transparentes »	57
Sous-chapitre 7.2.	Gestion des conflits d'intérêts	58
Section 7.2.1.	Exigences additionnelles relatives aux conflits d'intérêts en relation avec des parties liées	59
Sous-chapitre 7.3.	Procédure d'approbation des nouveaux produits (et des nouvelles activités) (« New Product Approval Process »)	60
Sous-chapitre 7.4.	Sous-traitance (« Outsourcing »)	61
Section 7.4.1.	Exigences générales en matière de sous-traitance	61
Section 7.4.2.	Exigences particulières en matière de sous-traitance dans le domaine informatique	63
Sous-section 7.4.2.1.	Services de gestion/d'opération des systèmes informatiques	64
Sous-section 7.4.2.2.	Services de conseil, de développement et de maintenance	64
Sous-section 7.4.2.3.	Services d'hébergement et propriété de l'infrastructure	65
Section 7.4.3.	Exigences générales supplémentaires	66
Section 7.4.4.	Documentation	67
Chapitre 8.	Reporting légal	68
Partie III.	Gestion des risques	68
Chapitre 1.	Principes généraux en matière de mesure et de gestion des risques	68
Sous-chapitre 1.1.	La gestion des risques	68
Sous-chapitre 1.2.	La mesure des risques	69
Chapitre 2.	Risques de concentration	69

<u>Chapitre 3. Risque de crédit</u>	<u>70</u>
<u>Sous-chapitre 3.1. Principes généraux</u>	<u>70</u>
<u>Sous-chapitre 3.2. Crédits immobiliers résidentiels aux particuliers</u>	<u>71</u>
<u>Sous-chapitre 3.3. Crédits aux promoteurs immobiliers</u>	<u>72</u>
<u>Chapitre 4. Tarification du risque (« Risk Transfer Pricing »)</u>	<u>73</u>
<u>Chapitre 5. Gestion patrimoniale privée (« banque privée »)</u>	<u>73</u>
<u>Chapitre 6. Risques liés aux entités shadow banking</u>	<u>74</u>
<u>Sous-chapitre 6.1. Mise en œuvre de principes de contrôle interne solides</u>	<u>75</u>
<u>Sous-chapitre 6.2. Application de limites quantitatives</u>	<u>75</u>
<u>Chapitre 7. Risque de charge pesant sur les actifs (« asset encumbrance »)</u>	<u>77</u>
<u>Chapitre 8. Risque de taux d'intérêt inhérent aux activités autres que de négociation</u>	<u>78</u>
<u>Partie IV. Entrée en vigueur, mesures transitoires et dispositions abrogatoires</u>	<u>78</u>

## 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. Le terme n'est pas à prendre dans son acception juridique, puisque les banques et entreprises d'investissement peuvent revêtir une forme juridique qui ne prévoit pas de « conseil d'administration » au sens du droit des sociétés. Par exemple, en présence d'un conseil de surveillance, ce dernier assumera les responsabilités que la présente circulaire attribue au « conseil d'administration » ;~~
- 2) ~~« direction autorisée » : les personnes visées aux articles 7 paragraphe 2 et 19 paragraphe 2 de la loi du 5 avril 1993 relative au secteur financier. Ces personnes sont désignées par « directeurs autorisés » ;~~
- 3) ~~« établissement » : une entité telle que définie au chapitre 2 de la partie I ;~~
- 4) ~~« fonction clé » : toute fonction dont l'exercice permet d'avoir une influence notable sur la conduite ou le contrôle des activités. Ces fonctions clé comprennent au minimum les administrateurs, directeurs autorisés et les responsables des trois fonctions de contrôle interne suivant le point 105 (c'est-à-dire la fonction de contrôle des risques, la fonction compliance et la fonction d'audit interne) ;~~
- 5) ~~« LSF » : la loi du 5 avril 1993 relative au secteur financier ;~~
- 6) ~~« parties liées » : les entités juridiques appartenant au groupe auquel l'établissement appartient ainsi que les employés, actionnaires, directeurs et membres du conseil d'administration de ces entités.~~

## **Chapitre 2. Champ d'application**

1) La présente circulaire s'applique aux établissements de crédit et aux entreprises d'investissement de droit luxembourgeois, y compris à leurs succursales, ainsi qu'aux succursales luxembourgeoises d'établissements de crédit et d'entreprises d'investissement dont l'origine se situe en dehors de l'Espace économique européen. Pour les domaines où la CSSF conserve une responsabilité de contrôle en tant qu'autorité d'accueil « autorité compétente » : la Banque centrale européenne (« BCE ») pour les établissements de crédit importants (« significant institutions », « SI ») ou la Commission de Surveillance du Secteur Financier (« CSSF ») pour les établissements de crédit moins importants (« less significant institutions », « LSI »)<sup>4</sup> et les succursales établies au Luxembourg d'établissements de crédit de pays tiers.

La CSSF conserve par ailleurs en tant qu'autorité d'accueil — il s'agit des mesures en matière de lutte contre le blanchiment des succursales luxembourgeoises d'établissements de crédit agréés dans un autre Etat membre une responsabilité de contrôle de certains domaines non liés à la surveillance prudentielle bancaire, à savoir notamment la lutte contre le blanchiment de capitaux et le financement du terrorisme, de marchés d'instruments financiers et de la liquidité — les règles applicables à la fourniture de services d'investissement et le contrôle des obligations applicables aux dépositaires d'OPC luxembourgeois.

2) « direction autorisée » ou « directeurs autorisés » : la direction autorisée est assimilée à l'organe de direction dans sa fonction exécutive selon les orientations de l'EBA en matière de gouvernance interne (Guidelines on internal governance « EBA/GL/2017/11 »). Les directeurs autorisés correspondent aux personnes visées à l'article 7 paragraphe 2 de la LSF et à la direction générale, telle que définie à l'article 3 du CRD IV.

D'un point de vue prudentiel, la direction autorisée est responsable de la gestion journalière d'un établissement, conformément aux orientations stratégiques et politiques clés approuvées par l'organe de surveillance. Dans un système moniste, les directeurs autorisés peuvent être également membres du conseil d'administration, alors que dans un système dualiste, la direction autorisée correspond strictement au directoire ;

<sup>4</sup> Conformément aux dispositions du Règlement UE N° 1024/2013 du Conseil du 15 octobre 2013 (« règlement MSU ») confiant à la BCE des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et du Règlement UE N° 468/2014 de la Banque centrale européenne établissant le cadre de la coopération au sein du mécanisme de surveillance unique entre la Banque centrale européenne, les autorités compétentes nationales et les autorités désignées nationales (« règlement-cadre MSU »).

- 3) « établissement » : les établissements de crédit de droit luxembourgeois, y compris leurs succursales, les succursales luxembourgeoises d'établissements de crédit et d'entreprises d'investissement originaires de pays tiers ainsi que les succursales luxembourgeoises d'établissements de crédit agréés dans un autre Etat membre ;
- 4) « établissement d'importance significative » : les établissements de crédit d'importance systémique suivant l'article 59-3 de la LSF et, le cas échéant, les autres établissements de crédit déterminés par l'autorité compétente sur base de l'évaluation de la taille et de l'organisation interne des établissements ainsi que de la nature, de l'échelle et de la complexité de leurs activités ;
- 5) « 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 orientations de l'EBA en matière de gouvernance interne (Guidelines on internal governance « EBA/GL/2017/11 »). Il désigne le conseil d'administration et la direction autorisée d'un Etat membre de l'Espace économique européen établissement pourvu d'une organisation moniste ou le conseil de surveillance et le directoire d'un établissement pourvu d'une organisation dualiste ;
- 6) « organe de surveillance » : l'organe de surveillance correspond à l'organe de direction dans sa fonction de surveillance selon les orientations de l'EBA en matière de gouvernance interne (Guidelines on internal governance « EBA/GL/2017/11 ») et aux membres de l'organe de direction qui n'exercent pas de fonction exécutive au sens de la LSF. La réglementation du secteur financier alloue aux conseils d'administration et aux conseils de surveillance des établissements de crédit des responsabilités en matière de surveillance et de contrôle, ainsi qu'en matière de détermination et d'approbation des orientations stratégiques et des principes directeurs ;
- 7) « parties liées » : les entités (structures) juridiques appartenant au groupe auquel l'établissement appartient ainsi que les membres du personnel, actionnaires et membres de l'organe de direction de ces entités ;
- 8) « Procédure prudentielle » : procédure prudentielle de nomination des membres de l'organe de direction et des titulaires de fonctions clés auprès des établissements de crédit ;
- 9) « 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 ;
- 10) CEBS : Committee of European Banking Supervisors ;

- 11) CRDIV : Directive 2013/36/UE du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE ;
- 12) CRR : le règlement européen n° 575/2013 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement ;
- 13) EEE : Espace Economique Européen ;
- 14) ICAAP : Internal Capital Adequacy Assessment Process ;
- 15) ILAAP : Internal Liquidity Adequacy Assessment Process ;
- 16) LSF : la loi modifiée du 5 avril 1993 relative au secteur financier ;
- 17) MiFID : Markets in Financial Instruments Directive.

## **Chapitre 2. Champ d'application et proportionnalité**

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

Pour les domaines où la CSSF conserve une responsabilité de contrôle en tant qu'autorité d'accueil, respectivement en tant qu'autorité en charge d'un domaine ne faisant pas partie de la surveillance prudentielle bancaire - il s'agit notamment des mesures en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, des règles applicables en matière de fourniture de services d'investissement et des obligations applicables aux dépositaires d'OPC luxembourgeois - les succursales luxembourgeoises d'établissements de crédit agréés dans un autre Etat membre mettent en place en coordination avec cet établissement agréé un dispositif en matière d'administration centrale et de gouvernance interne ainsi qu'une gestion des risques qui sont comparables à ceux prescrits par la présente circulaire.

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

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

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

2-3. La circulaire s'applique aux établissements sur une base individuelle, sous-consolidée et consolidée-, aux compagnies financières holding ou aux compagnies financières holding mixtes visées à l'article 21a (1) de la CRD IV et aux établissements de crédit visés à l'article 21a (4) c) de la CRD IV.

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

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

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 ~~de ces activités et des~~ risques.

~~3.-~~ 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 ~~des de leurs~~ activités, y compris les risques, ~~et de l'organisation de l'établissement.~~

En pratique, l'application du principe de proportionnalité conduit les établissements qui sont plus importants, complexes ou risqués à se doter d'un dispositif renforcé en matière d'administration centrale ~~et~~ de gouvernance interne et de gestion des risques. Ce dispositif renforcé comprend par exemple, l'instauration de comités spécialisés ~~suivant,~~ la section 4.1.4. nomination de membres indépendants additionnels à l'organe de surveillance ou encore de directeurs autorisés supplémentaires pour faciliter la gestion journalière.

A l'opposé, pour des établissements dont la ~~diversité, la taille ou l'organisation interne ainsi que~~ la nature, l'échelle et la complexité de l'activité des activités sont moindres, le principe de proportionnalité peut jouer à la baisse. Ainsi ~~ces établissements peuvent, un établissement ayant des activités limitées et peu complexes peut~~ fonctionner adéquatement au sens de la présente circulaire avec en désignant des responsables des fonctions compliance et de contrôle des risques ~~assumées~~ à temps partiel (~~voir les points 129 et 141~~), ~~avec un audit interne sous-traité (point 117)~~ sans remettre en cause le principe de permanence de la fonction ou ~~encore moyennant le recours à des experts externes en vue de réaliser certaines en sous-traitant l'exécution des~~ tâches opérationnelles de contrôle-l'audit interne (point 118) 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 (~~voir le point 71~~).

Au niveau de la direction autorisée, ~~ce principe est atténué par le principe de la responsabilité collective de la direction autorisée (voir le point 72)~~ alors que la répartition des tâches ~~au niveau de la direction autorisée~~ s'effectue dans le respect du principe de la ségrégation des tâches, la responsabilité reste collective. ~~Par application du principe de proportionnalité, lorsqu'un établissement ne nécessite pas plus que deux directeurs autorisés, la répartition efficace des tâches n'est pas toujours compatible avec une ségrégation stricte des tâches au niveau de cette direction. Par exemple, il est admissible dans ce cas de figure que le même membre de la direction autorisée soit en charge à la fois de l'organisation administrative, comptable et informatique et des fonctions de contrôle interne (voir le point 63).~~

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 ~~au chapitre 3 de la partie II.~~ 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 l'organe de surveillance.

## 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. ~~La notion de Le~~ centre de prise de décision ~~ne comprend pas seulement l'activité de~~ la direction autorisée ~~suivant ainsi que~~ les ~~articles 7 paragraphe 2 et 19 paragraphe 2 de la LSF, mais également celle des~~ responsables des ~~différentes~~ fonctions commerciales, des fonctions de support et de contrôle ~~ou et~~ des différentes unités opérationnelles ~~(services, départements ou métiers)~~ existant à l'intérieur de l'établissement.
3. Le centre administratif comprend ~~en particulier une bonne organisation~~ 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 ~~délais. Il inclut à ce titre l'infrastructure administrative des fonctions commerciales (section 5.2.1), les fonctions de support, en particulier dans le domaine financier et comptable (section 5.2.2) et informatique (section 5.2.3), ainsi que le contrôle interne (chapitre 6).~~ délai.
4. Lorsque l'établissement est tête de groupe ~~suivant le point 3~~, l'administration centrale permet à l'établissement de concentrer en son siège à Luxembourg toute l'information de gestion nécessaire pour gérer, suivre et contrôler de façon continue les activités du groupe. De même, l'administration centrale permet à l'établissement d'atteindre toutes les entités juridiques et succursales qui composent le groupe afin de leur fournir toute l'information de gestion nécessaire. La notion d'information de gestion s'entend au sens le plus large, incluant l'information financière et le reporting ~~prudentiel~~ légal.

## Chapitre 2. Le dispositif de gouvernance interne

5. La gouvernance interne est une composante ~~limitée mais~~ cruciale de la gouvernance d'entreprise, se concentrant sur la structure interne et l'organisation d'un établissement. La gouvernance d'entreprise est un concept plus vaste qui peut être décrit comme étant l'ensemble des relations entre un établissement, son ~~conseil d'administration~~ organe de surveillance, sa direction autorisée, ses actionnaires et les autres parties prenantes.

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

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

~~— «° La seconde ligne est formée par les fonctions de support, y compris la fonction financière et comptable (section 5.2.2 de la présente circulaire), et les fonctions compliance et de contrôle des risques (sous-chapitre 6.2 et sections 6.2.5 et 6.2.6 de la présente circulaire, et orientation 1.3<sup>5</sup> mises en œuvre par la circulaire CSSF 20/750 pour le cadre de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité) qui contribuent au contrôle indépendant des risques.°»<sup>6</sup>~~

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

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

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

~~<sup>5</sup> Orientation 3.3 dans la version anglaise.~~

~~<sup>6</sup> Modifié par la circulaire CSSF 20/750~~

- une structure organisationnelle et opérationnelle claire et cohérente comportant des pouvoirs de décision, des liens hiérarchiques et fonctionnels et un partage des responsabilités clairement définis, transparents, cohérents, complets et exempts de conflits d'intérêts ~~(sous chapitres 5.1, 7.1 et 7.2)~~ ;
- des mécanismes adéquats de contrôle interne qui répondent aux dispositions du chapitre 6 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 ~~par application des règles contenues dans les circulaires CSSF 06/273, CSSF 07/290 et CSSF 11/505~~, en ligne avec la stratégie de l'établissement en matière de risques, ainsi que des mécanismes de contrôle et de sécurité des systèmes d'information de gestion. La notion de système d'information de gestion comprend les systèmes informatiques ~~(sections 5.2.1 à 5.2.3, sous chapitres 5.3 et 7.4)~~ ;
- ~~une procédure formelle d'escalade, de règlement et, le cas échéant, de sanctions pour les problèmes, déficiences et irrégularités relevés par le biais des mécanismes de contrôle interne, y compris les fonctions de contrôle interne suivant le sous-chapitre 6.2 ;~~
- 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 ~~et~~ d'atténuation ~~ainsi que et~~ de contrôle des risques auxquels les établissements sont ou pourraient être exposés ~~conformément au chapitre 1 de la partie III~~ ;
- un système d'information de gestion, y compris en matière de risques, ainsi qu'un dispositif de communication interne comprenant un dispositif interne d'alerte (« whistleblowing ») qui permet au personnel de l'établissement d'attirer l'attention des responsables sur toutes leurs préoccupations importantes et légitimes liées à la gouvernance interne de l'établissement (section 5.2.4) ;
- 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 ~~et~~ clés telles que définies par ~~le conseil d'administration l'organe de surveillance~~ sur proposition de la direction autorisée. Ce dispositif comprend un plan de continuité qui décrit les actions à mettre en œuvre afin de poursuivre les activités en cas d'incident ou sinistre ~~(sections 5.2.3 et 7.4)~~ ;
- un dispositif de gestion de crises qui assure une capacité de réaction appropriée en cas de crise, y compris un plan de ~~rétablissement des activités. Ce dispositif satisfait redressement conforme~~ aux exigences ~~énoncées à du~~ chapitre 2 de la section 5.2.5 partie IV de la LSF.

7. ~~Les établissements promeuvent~~ Tout établissement promeut une culture interne du ~~contrôle et 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 ~~tel que défini au chapitre 6.~~

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 l'organe de direction (« 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, ~~les établissements tout établissement~~ se ~~dotent-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 ~~(nécessairement)~~ au seul périmètre (consolidé) prudentiel ou comptable<sup>1</sup>. Il doit permettre à l'établissement de disposer d'une vue exhaustive sur tous ses risques, en termes de ~~leur~~ substance économique, en tenant compte de toutes les interactions existant à travers l'établissement. S'agissant du contrôle interne, le principe d'exhaustivité implique que le contrôle interne porte sur tous les domaines du fonctionnement de l'établissement ;

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

~~9. En exécution d'un organigramme (sous-chapitre 5.1), l'établissement dispose au siège luxembourgeois, dans ses succursales ainsi que dans l'ensemble des différentes entités juridiques qui composent le groupe, de ressources humaines suffisantes en nombre et disposant d'une compétence professionnelle individuelle et collective appropriée, ainsi que de l'infrastructure administrative et technique nécessaire et suffisante pour pouvoir exercer les activités qu'il veut réaliser. Ces ressources humaines et cette infrastructure respectent les dispositions des sous-chapitres 5.1 et 5.2.~~

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

~~10. Les établissements documentent par écrit l'ensemble du dispositif en matière d'administration centrale et de gouvernance interne ainsi que l'ensemble de leurs activités (opérations et risques) conformément au sous-chapitre 5.3.~~

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

~~11.9.~~ 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.

~~12.10.~~ Les établissements publient les éléments clés de leur dispositif clés en matière de gouvernance interne et de gestion des règles régissant la partie ~~XIX~~ risques conformément aux dispositions du CRR (article 435 et titre I<sup>er</sup> de la circulaire CSSF 06/273 (« pilier 3 »). Cette huitième partie) ainsi qu'aux orientations relatives aux exigences de publication inclut ~~la~~ la structure organisationnelle et opérationnelle, y compris en matière de contrôle interne, la stratégie en matière de risques ainsi que le profil l'EBA (Guidelines on disclosure requirements under part eight of regulation (EU) no 575/2013, « EBA/GL/2016/11 ») de risque. Ces informations décrivent la situation actuelle et son évolution attendue d'une manière claire, objective et pertinente.

## Chapitre 4. ~~Conseil d'administration~~ Organe de surveillance et direction autorisée

Sous-chapitre 4.1. ~~Le conseil d'administration~~ L'organe de surveillance

### **Section 4.1.1. Responsabilités ~~du conseil d'administration de~~ l'organe de surveillance**

~~13-11. Le conseil d'administration~~ L'organe de surveillance a la responsabilité globale de l'établissement. Il ~~veille à faire assurer l'activité définit, surveille et à préserver~~ porte la continuité-responsabilité de l'activité au moyen la mise en place d'un solide dispositif en matière d'administration centrale ~~et de gouvernance interne conformément aux dispositions de la présente circulaire, 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~~ l'organe de surveillance approuve et arrête par écrit, ~~dans le respect des dispositions légales et réglementaires et~~ après avoir entendu la direction autorisée et les responsables des fonctions de contrôle interne, ~~et dans le but de protéger l'établissement les éléments clés suivants du dispositif en matière d'administration centrale, de gouvernance interne et sa réputation, notamment de gestion des risques :~~

- la stratégie commerciale (modèle ~~d'activités d'affaires~~) de l'établissement dans le respect des intérêts financiers de l'établissement à long terme, de sa solvabilité ~~et de sa situation des liquidités, 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 ~~la tolérance l'appétit au risque et les principes directeurs régissant la détection, la mesure, la déclaration, la le cadre global de prise et de gestion et le contrôle~~ des risques de l'établissement ;
- la stratégie de l'établissement en matière de fonds propres et de réserves de liquidités réglementaires et internes ;
- ~~les principes directeurs d'une~~ une structure organisationnelle et opérationnelle claire et cohérente qui règle en particulier la création et le maintien par l'établissement d'entités (structures) juridiques, ~~ainsi que les principes directeurs en matière de systèmes d'informations, y compris l'aspect sécurité, et de dispositif de communication interne, y compris le dispositif interne d'alerte ;~~

- les principes directeurs 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 ~~et la~~ ;
- 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, ~~de règlement~~ et de sanctions visant à assurer que tout comportement non respectueux ~~de des~~ règles applicables soit adéquatement poursuivi et sanctionné, ~~ainsi que les principes directeurs en matière de déontologie (« code de conduite interne ») et de valeurs d'entreprise, y compris dans le domaine de la gestion des conflits d'intérêts ;~~
- les principes directeurs en matière d'administration centrale au Luxembourg, comprenant :
  - les moyens humains et matériels que nécessite la mise en œuvre de la structure organisationnelle et opérationnelle ainsi que des stratégies de l'établissement, ~~les principes directeurs en matière d'organisation~~
  - 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 ~~se~~ 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 ~~applicables~~ en matière de ~~dispositif de gestion de~~ continuité des activités et de gestion de crises ~~et~~ ;

- les principes directeurs régissant la nomination et la succession à l'organe de direction et aux fonctions élé-clés de l'établissement, ainsi que les procédures régissant le conseil d'administration l'organe de surveillance en termes de sa composition, de ses comprenant les aspects de diversité, de responsabilités, de son organisation et d'organisation, de son fonctionnement et d'évaluation individuelle et collective de ses membres.<sup>7</sup> Les principes directeurs régissant la nomination et la succession aspects de diversité font référence aux fonctions clé de l'établissement stipulent qu'en la matière, l'établissement doit se conformer aux exigences de la présente circulaire, à la procédure prudentielle d'approbation caractéristiques des titulaires membres de fonctions clé telle que publiée l'organe de direction, y compris leur âge, sexe, origine géographique et parcours éducatif et professionnel. La promotion de la diversité repose sur le site internet de la CSSF ainsi qu'aux orientations publiées par l'EBA le 22 novembre 2012 (Guidelines on the assessment of the suitability of members of the management body and key function holders — EBA/GL/2012/06). principe de non-discrimination et sur des mesures garantissant l'égalité des chances.

14.12. Le conseil d'administration L'organe de surveillance charge la direction autorisée de mettre en œuvre les stratégies et principes directeurs en matière de gouvernance interne visés au point 17 par le biais de politiques et de procédures internes écrites, (à l'exception des principes directeurs qui régissent la nomination et la succession au conseil d'administration sein de l'organe de surveillance et les procédures déterminant son fonctionnement).

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

16.14. Le conseil d'administration L'organe de surveillance évalue d'une manière critique et approuve, adapte en cas de besoin et réapprouve à des intervalles réguliers, et au moins une fois par an, le dispositif de gouvernance interne de l'établissement, 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.

<sup>7</sup> Dans le respect de la gouvernance d'entreprise, les principes directeurs et procédures applicables aux membres de l'organe de surveillance sont à soumettre, le cas échéant aux actionnaires pour accord, dans le respect de la procédure prudentielle, telle que publiée sur le site de la CSSF.

L'évaluation et ~~l'approbation~~ la ré-approbation par ~~le conseil d'administration~~ l'organe de surveillance 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~~ l'organe de surveillance et la réglementation ~~existante et notamment applicable, y compris~~ la circulaire CSSF 11/506 ;
- les stratégies et principes directeurs en vue de les améliorer et de les adapter aux changements internes et externes, actuels et anticipés, ainsi qu'aux enseignements tirés du passé ;
- la manière dont la direction autorisée s'acquitte ~~des responsabilités énoncées au sous-chapitre 4.2. Dans ce contexte, le conseil d'administration de ses responsabilités et les performances de ses membres. Dans ce contexte, l'organe de surveillance 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 et ~~la CSSF, conformément aux deux derniers paragraphes du point 57~~ l'autorité compétente ;
- l'adéquation de la structure organisationnelle et opérationnelle. ~~Le conseil d'administration~~ L'organe de surveillance 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 relie ainsi que des risques y liés. Il vérifie que la structure organisationnelle et opérationnelle correspond aux stratégies et principes directeurs ~~visés au point 17~~, qu'elle permet une gestion saine et prudente des activités qui est exempte d'opacité et de complexité indue, et qu'elle reste justifiée par rapport aux objectifs assignés. Cette exigence s'applique tout particulièrement aux activités ~~« inhabituelles »~~ ou ~~« 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 ~~mis en place par application du point 33~~ spécialisés. Elles se font en particulier sur base des informations reçues de la part de la direction autorisée ~~(point 61)~~, des rapports de révision émis par le réviseur d'entreprises agréé (rapports sur les comptes annuels, comptes rendus analytiques et, le cas échéant, « management letters »), ~~du rapport des rapports ICAAP (point 61), ILAAP~~ et des rapports ~~de synthèse~~ des fonctions de contrôle interne ~~(point 116)~~ que ~~le conseil d'administration~~ l'organe de surveillance est appelé à approuver à cette occasion.

~~17-15.~~ Il appartient ~~au conseil d'administration à l'organe de surveillance~~ 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 l'organe de surveillance~~ veille à ce que les travaux de ces fonctions soient exécutés suivant des normes reconnues. ~~Par ailleurs, le conseil d'administration approuve le plan d'audit interne conformément au point 151, et dans le cadre de politiques approuvées.~~

16. L'organe de surveillance veillera à consacrer un temps suffisant aux thématiques du risque.

~~18-17.~~ Lorsque ~~le conseil d'administration l'organe de surveillance~~ prend connaissance que le dispositif en matière d'administration centrale ou de gouvernance interne ne permet plus une gestion saine et prudente des activités ou que les risques encourus ne sont ou ne seront plus adéquatement supportés par la capacité de l'établissement à gérer ces risques, par des fonds propres ou des réserves de liquidités réglementaires ou internes, il exige de la direction autorisée de lui présenter sans délais des mesures correctrices et en ~~informe~~ notifie immédiatement ~~la CSSF l'autorité compétente~~. L'obligation de notification à ~~la CSSF l'autorité compétente~~ porte aussi sur toutes les informations qui remettent en cause la qualification ou l'honorabilité ~~d'un membre du conseil d'administration de membres de l'organe de direction~~ ou de la direction autorisée ou d'un responsable d'une fonction ~~de contrôle interne clé~~.

#### **Section 4.1.2. Composition et qualification ~~du conseil d'administration de l'organe de surveillance~~**

~~19-18.~~ Les membres ~~du conseil d'administration de l'organe de surveillance~~ doivent être suffisants en nombre et présenter dans leur ensemble une composition adéquate qui permet ~~au conseil d'administration à l'organe de surveillance~~ de s'acquitter pleinement de toutes ses responsabilités. Le caractère adéquat se réfère en particulier aux ~~compétences qualités~~ compétences professionnelles (connaissances, ~~compréhension~~ compétences et expérience adéquates), ainsi qu'aux qualités personnelles des membres ~~du conseil d'administration de l'organe de surveillance~~. Par ailleurs, chaque membre doit justifier son honorabilité professionnelle. Les principes directeurs régissant ~~l'élection la nomination~~ la nomination et la succession des ~~administrateurs membres de l'organe de surveillance~~ expliquent et arrêtent les facultés jugées nécessaires en vue d'assurer une composition et une qualification ~~appropriée du conseil d'administration appropriées de l'organe de surveillance~~.

~~20-19.~~ L'organe de surveillance doit disposer ~~dans son ensemble collectivement de connaissances, compétences et d'une compétence appropriée 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, en tant que collectif,~~ L'organe de surveillance 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 de l'organe de surveillance~~ 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.

~~21-20.~~ Les membres ~~du conseil d'administration de l'organe de surveillance~~ veillent à ce que leurs qualités personnelles leur permettent d'exécuter leur mandat ~~d'administrateur~~ de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit requis. A ce titre, ~~le conseil d'administration l'organe de surveillance~~ ne peut pas compter parmi ses membres une majorité de personnes qui assument un rôle exécutif au sein de l'établissement (directeurs autorisés ou autres employés-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 de l'organe de surveillance~~ veillent à ce que leur mandat ~~d'administrateur~~ 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 l'organe de surveillance~~ des mandats qu'ils ont en dehors de l'établissement.

~~22-21.~~ Les termes des mandats ~~d'administrateur~~ doivent être fixés de manière à permettre ~~au conseil d'administration à l'organe de surveillance~~ d'exercer ses responsabilités de manière continue et efficace. La reconduction ~~d'administrateurs de membres~~ existants doit s'orienter en particulier à leurs performances passées. La continuité du fonctionnement ~~du conseil d'administration de l'organe de surveillance~~ doit être assurée.

22. Les principes directeurs régissant la nomination et la succession des membres ~~du conseil d'administration de l'organe de surveillance~~ 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 formations professionnelles programmes de formation professionnelle qui permettent aux membres ~~du conseil d'administration de mettre de l'organe de surveillance 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 ~~requis~~.

23. Chaque établissement devrait nommer au moins un membre à son organe de surveillance qui peut être considéré comme « membre indépendant ».

Un membre indépendant de l'organe de surveillance 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 organe de surveillance 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 de l'organe de surveillance~~***

24. ~~Le conseil d'administration~~ ~~L'organe de surveillance~~ se réunit régulièrement en vue de s'acquitter de manière efficace de ses responsabilités. L'organisation et le fonctionnement de l'organe de surveillance 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 de l'organe de surveillance~~ doivent être documentés par écrit. Cette documentation inclut l'agenda ~~des réunions, et~~ les procès-verbaux des réunions ~~ainsi que avec~~ les décisions et mesures prises par ~~le conseil d'administration~~ l'organe de surveillance. Les procès-verbaux sont un outil important qui doit aider l'organe de surveillance et ses membres à faire le suivi des décisions d'une part, et permettre à l'organe et à ses membres de rendre des comptes aux actionnaires et aux autorités compétentes, 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~~ L'organe de surveillance évalue régulièrement les procédures régissant ~~le conseil d'administration~~, son mode de fonctionnement et ses travaux en vue de les améliorer, d'en assurer l'efficacité et de vérifier si les procédures qui lui sont applicables sont respectées dans la pratique. 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 de l'organe de surveillance et des comités spécialisés qui en dépendent.
27. Il appartient au président ~~du conseil d'administration de l'organe de surveillance~~ 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 de l'organe de surveillance~~ une culture de discussion informée et contradictoire et de proposer l'élection d'administrateurs la nomination de membres indépendants. Un administrateur indépendant est un administrateur qui ne connaît ~~Le président de l'organe de surveillance n'exerce pas de conflit d'intérêts, de nature à altérer sa capacité de jugement du fait qu'il est lié par une relation d'affaires familiale ou autre<sup>6</sup> avec fonctions exécutives au sein de l'établissement, l'actionnaire qui le contrôle ou la direction de l'un ou de l'autre~~ hormis situations exceptionnelles à autoriser par l'autorité compétente.
- ~~La CSSF recommande aux grands établissements d'avoir un ou plusieurs administrateurs indépendants.~~
28. ~~Les mandats de directeur autorisé et de président du conseil d'administration ne sont pas cumulables.~~

<sup>6</sup> ~~Y inclus une relation salariale~~

#### **Section 4.1.4. Comités spécialisés**

~~28. En vue d'accroître son efficacité, le conseil d'administration~~  
L'organe de surveillance peut se faire assister par des comités spécialisés dans ~~le domaine~~ les domaines notamment de l'audit, des risques, de la compliance, de la rémunération, ~~et~~ des ressources humaines (notamment à travers l'intervention d'un ~~comité de nomination des personnes occupant une fonction clé~~) ainsi que nominations ou encore de la gouvernance interne, ~~et~~ de la déontologie, en fonction de ses besoins et compte tenu de l'organisation, de la ~~compliance lorsque la~~ nature, ~~de~~ l'échelle et ~~de~~ la complexité ~~de l'établissement et de ses~~ des activités l'exigent. Ces comités comprennent des administrateurs qui ne font pas partie de la direction autorisée ni du personnel de l'établissement. Ils peuvent également comprendre, au besoin, des experts externes, indépendants de l'établissement. Leur mission consiste de l'établissement. Leurs missions consistent à fournir ~~au conseil d'administration à~~ l'organe de surveillance des appréciations critiques concernant l'organisation et le fonctionnement de l'établissement dans ~~les domaines précités en vue de permettre aux membres du conseil d'administration d'exercer de manière efficace leur mission de surveillance et d'assumer leurs~~ 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.

~~29-30.~~ 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 en vertu de la présente circulaire, 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.

~~30.~~ Le conseil d'administration fixe par écrit le mandat, la composition et les procédures de travail des comités spécialisés. En vertu de ces procédures, les comités spécialisés doivent pouvoir demander tout document et toute information qu'ils jugent utiles pour l'exercice de leur mission. Par ailleurs, les procédures prévoient les conditions dans lesquelles le réviseur d'entreprises agréé ainsi que toute personne appartenant à l'établissement, y compris la direction autorisée, sont associés aux travaux des comités spécialisés.

~~31. Le conseil d'administration veille à ce que les différents comités interagissent efficacement et rapportent régulièrement au conseil d'administration. Le conseil d'administration ne peut pas déléguer aux comités spécialisés ses pouvoirs de décision et responsabilités en vertu de la présente circulaire.~~

31. Sans préjudice d'exigences légales et réglementaires spécifiques en la matière, les membres permanents des comités spécialisés sont, selon le cas, des membres de l'organe de surveillance 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 de l'organe de surveillance 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. Lorsque le conseil d'administration~~ 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 de l'organe de surveillance. 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. L'organe de surveillance 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. L'organe de surveillance 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 à l'organe de surveillance.

~~33-37.~~ L'organe de surveillance ne peut pas déléguer aux comités spécialisés ses pouvoirs et responsabilités en vertu de la présente circulaire. Lorsqu'il ne se fait pas assister par des comités spécialisés, les tâches énoncées aux sous-sections 4.1.4.1 et 4.1.4.2 lui incombent directement au conseil d'administration.

#### *Sous-section 4.1.4.1. Le comité d'audit*

~~34-38.~~ Le comité d'audit a pour objet d'assister le conseil d'administration-l'organe de surveillance 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.

~~35-39.~~ La CSSF recommande aux grands-Sans préjudice des autres dispositions de la section 4.1.4, les établissements de-doivent créer un comité d'audit afin de faciliter le contrôle effectif des activités lorsqu'ils y sont tenus par le conseil d'administration, l'article 52 de la loi modifiée du 23 juillet 2016 relative à la profession de l'audit (« Loi Audit »).

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

~~36. Le fonctionnement du comité d'audit, en particulier en termes de fréquence et de durée des réunions, est déterminé en fonction de son mandat et de sa mission d'assister le conseil d'administration.~~

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

~~37-41. Le comité d'audit confirme la charte d'audit interne (point 144) 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 nécessaires (point 111) et que l'indépendance de la fonction d'audit interne est sauvegardée en nécessaires.~~

~~38. Le comité d'audit confirme le plan d'audit interne (point 151) approuvé par la direction autorisée. Il prend connaissance des informations sur l'état du contrôle interne que lui fournit la direction autorisée selon une fréquence au moins annuelle en vertu du point 61 de la présente circulaire.~~

~~39-42. Le comité d'audit délibère régulièrement sur et de manière critique sur les sujets suivants<sup>9</sup> :~~

- ~~• le suivi du 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 dans la présente circulaire (voir sections 6.2.3. et 6.2.7.3), ;~~
- ~~• la nomination, la reconduction, la révocation et la rémunération du réviseur d'entreprises agréé,~~
- ~~• la qualité du travail réalisé par le réviseur d'entreprises agréé, son indépendance et objectivité, son respect des règles déontologiques en vigueur dans le domaine ainsi que la portée et la fréquence d'audit. A ce titre, le comité d'audit analyse et évalue d'une manière critique le plan d'audit, les rapports sur les comptes annuels, les « management letters » ainsi que, les comptes rendus analytiques réalisés 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 et assure un examen et suivi de l'indépendance du réviseur d'entreprises agréé ou du cabinet de révision agréé, en particulier pour ce qui concerne la fourniture de services complémentaires à l'établissement, ;~~

<sup>9</sup> 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.

- le suivi approprié et sans délai indu par la direction autorisée des recommandations de la fonction d'audit interne et du réviseur d'entreprises agréé ~~destinées à améliorer l'organisation et le contrôle interne, et les actions entreprises pour remédier aux problèmes, déficiences et irrégularités relevés.~~
- ~~les actions~~ En rendant compte à prendre en cas l'organe de surveillance dans son ensemble, le comité d'audit propose les mesures nécessaires pour corriger rapidement les problèmes, déficiences et irrégularités constatés. relevés par le service d'audit interne et le réviseur d'entreprises agréé,
- ~~le respect des dispositions légales et statutaires ainsi que des règles CSSF pour l'établissement des comptes annuels individuels et, le cas échéant, consolidés, et sur la pertinence des méthodes comptables adoptées.~~

~~40-43. Il est admissible que~~ Le comité d'audit ~~couvre également le volet compliance sans qu'un comité informe l'organe de compliance à part soit constitué. Dans ce cas, le mandat et la composition~~ surveillance 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 reflètent ces nouvelles attributions. En particulier, les personnes associées au comité d'audit en vertu du point 39 incluent le « Chief Compliance Officer » suivant le point 105 dans ce processus.

#### *Sous-section 4.1.4.2. Le comité des risques*

~~41-44. Le comité des risques a pour objet d'assister le conseil d'administration dans sa mission d'évaluation de conseiller l'organe de surveillance 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.

~~42. La CSSF recommande aux grands~~ Les établissements de même qu'aux établissements présentant un profil de risque plus élevé ou complexe de d'importance significative doivent créer un comité des risques afin de faciliter, dans le contrôle effectif respect des risques par le conseil d'administration.

~~43-45. Le comité des risques peut associer à ses travaux la direction autorisée ainsi que les responsables des fonctions de contrôle interne. Ces personnes peuvent assister aux réunions~~ dispositions de l'article 7 du comité ; elles n'en sont pas membres RCSSF 15-02.

~~44-46. Le comité des risques confirme les politiques spécifiques de la direction autorisée suivant la section 4.1.1.2-3. de la partie III. Il assiste l'organe de surveillance 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.~~

~~45-47.~~ Le comité des risques apprécie si les moyens humains et matériels, ainsi que l'organisation de la fonction de contrôle des risques (~~section 6.2.5.~~) sont suffisants et s'assure que les membres de la fonction de contrôle des risques possèdent les compétences nécessaires.

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

~~46-49.~~ Le comité des risques délibère régulièrement et de manière critique sur les sujets suivants :

- ~~• l'état de la gestion des risques et le respect des règles prudentielles fixées à ce sujet,~~
- 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 (~~voir sous-chapitre 6.2.3 et section 6.2.5 en particulier~~); ;
- ~~• la situation des risques, son évolution future~~l'évaluation, par le biais de scénarios et son adéquation avec la stratégie de tests d'endurance, de l'influence d'événements externes et internes sur le profil de risque de l'établissement en matière et de risques;
- ~~• l'adéquation entre les risques encourus, la capacité actuelle et future de l'établissement à gérer ces risques et les fonds propres et réserves de liquidités internes et réglementaires, eu égard aux résultats de tests d'endurance suivant la circulaire CSSF 11/506,~~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 à prendre en cas de entreprises pour remédier aux problèmes, déficiences et irrégularités relevés par la fonction de contrôle des risques. ;
- Le comité des risques conseille le conseil d'administration 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 définition risques ;

- sans préjudice des responsabilités du comité de la stratégie globale 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 à l'organe de surveillance dans son ensemble du résultat de ses délibérations en matière de risques, y compris sa tolérance aux risques actuels et futurs, 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 de l'organe de surveillance ni d'aucun autre comité spécialisé.

Sous-chapitre 4.2. La direction autorisée

#### **Section 4.2.1. Responsabilités de la direction autorisée**

47-51. La direction autorisée est responsable pour 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 fixés approuvés par le conseil d'administration l'organe de surveillance et de la réglementation existante applicable, en prenant en considération et en préservant les intérêts financiers de l'établissement à long terme, sa solvabilité et sa situation des liquidités. Les décisions prises par la direction autorisée dans ces domaines sont dûment documentées. 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 à l'organe de surveillance et aux autorités compétentes 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.

48-52. Conformément aux articles à l'article 7 paragraphe 2 et 19, paragraphe 2 de la LSF, les membres de la direction autorisée doivent être habilités à déterminer effectivement l'orientation de l'activité. Par conséquent, lorsque des décisions de gestion sont prises par des comités de gestion plus larges que la seule direction autorisée, il est requis que qu'au moins un membre de la direction autorisée en fasse partie et qu'il existe un droit de veto à leur son bénéfice.

53. La direction autorisée exerce une fonction permanente à l'intérieur de l'établissement ; elle doit en principe se trouver de façon permanente sur place. Toute dérogation à ce principe doit être autorisée par la CSSF.

~~49-54.~~ 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~~ l'organe de surveillance 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, ~~et~~ les procédures sont les instructions de travail qui régissent cette mise en œuvre. Le terme « procédures » est à prendre au sens large, comprenant l'ensemble des mesures, instructions et règles qui régissent l'organisation et le fonctionnement interne.

~~Elle~~ La direction autorisée veille à ce que l'établissement dispose ~~de~~ 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.

~~50-55.~~ En application ~~du point 18 des principes directeurs en matière de déontologie, de valeurs d'entreprise et de gestion des conflits d'intérêts arrêtés par l'organe de surveillance,~~ 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 et aux membres de l'organe de direction 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.

~~51-56.~~ La direction autorisée doit avoir une compréhension parfaite de la structure organisationnelle et opérationnelle de l'établissement, en particulier en termes ~~des entités d'entités~~ (structures) juridiques sous-jacentes, de leur raison d'être, des liens et interactions intra-groupe qui les relie ainsi que des risques y liés. Elle veille à ce que les informations de gestion requises soient disponibles en temps utile à tous les niveaux de prise de décision et de contrôle de l'établissement et des ~~structures entités~~ juridiques qui le composent.

~~52-57.~~ Dans sa gestion journalière, la direction autorisée tient compte des conseils et avis formulés par les fonctions de contrôle interne.

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

La direction autorisée met en œuvre de manière prompte et efficace les mesures correctrices pour remédier aux faiblesses (problèmes, déficiences ~~et~~ irrégularités ou préoccupations) relevées par les fonctions de contrôle interne ~~et~~ le réviseur d'entreprises agréé ou par l'intermédiaire du dispositif d'alerte interne en prenant en compte ~~leurs-les~~ recommandations ~~en la matière~~ émises dans ce contexte. Cette manière de procéder est arrêtée dans une procédure écrite que ~~le conseil d'administration~~ l'organe de surveillance 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~~ l'organe de surveillance qui doit autoriser les prorogations ~~de-des~~ délais d'implémentation ~~des~~ mesures correctrices.

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

~~53-58.~~ 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.

~~54-59.~~ 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.

~~55-60.~~ La direction autorisée informe les fonctions de contrôle interne des changements majeurs en matière d'activités ~~(voir sous-chapitre 7.3)~~ ou d'organisation afin de leur permettre de détecter et d'évaluer les risques qui peuvent en résulter.

61. La direction autorisée informe, de manière complète et par écrit, régulièrement et au moins une fois par an, ~~le conseil d'administration~~ l'organe de surveillance 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 ~~le rapport les rapports~~ ICAAP/ILAAP sur la situation et la gestion des risques, des fonds propres et des ~~(réserves de)~~ liquidités réglementaires et internes.

~~56-62. Ces informations portent en particulier sur l'état du contrôle interne.~~ Une fois par an, la direction autorisée confirme à ~~la CSSF~~ l'autorité compétente le respect de la présente circulaire par le biais d'une phrase écrite unique suivie des signatures de toute la direction autorisée. Lorsqu'en raison d'un manque de conformité, la direction autorisée n'est pas en mesure de confirmer le respect intégral de la circulaire, la déclaration précitée prend la forme d'une réserve qui énonce sommairement les points de non-conformité en donnant des explications sur leurs raisons d'être.

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

57-63. 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~~ l'organe de surveillance et ~~la CSSF~~ l'autorité compétente en leur fournissant sans délai toute l'information nécessaire pour apprécier la situation ~~(voir également le point 22)~~.

58-64. Nonobstant la responsabilité collective des membres de la direction autorisée ~~(voir le point 72)~~, cette dernière désigne au moins un de ses membres qui est en charge de l'organisation administrative, comptable et informatique et qui assume la responsabilité de la mise en œuvre de la politique et des règles qu'elle a fixées dans ce domaine. ~~Il~~ Ce membre est responsable en particulier de l'établissement de l'organigramme et de la description des tâches ~~(voir le point 68)~~ qu'il soumet, avant leur mise en application, à l'approbation de la direction autorisée. Il veille ensuite à leur application correcte. Le membre en question est aussi responsable de la production et de la publication des informations comptables destinées aux tiers et de la communication des informations périodiques à ~~la CSSF~~ l'autorité compétente. Il veillera donc à ce que la forme et le contenu de ces informations soient conformes aux prescriptions légales et ~~de la CSSF~~ aux instructions de l'autorité compétente en la matière.

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

~~59-65.~~ Les établissements informent ~~la CSSF sur les personnes visées au point 105.~~ ~~La direction autorisée rapporte à la CSSF, par écrit et dans les meilleurs délais,~~ ~~les l'autorité compétente des~~ nominations et révocations ~~des membres~~ de ~~ees~~ ~~personnes~~ ~~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**

~~60-66.~~ Les membres de la direction autorisée possèdent, à la fois individuellement et collectivement, les ~~compétences~~ qualités professionnelles (connaissances, ~~compréhension~~ compétences et expérience), l'honorabilité et les qualités personnelles nécessaires pour gérer l'établissement et déterminer effectivement l'orientation de son activité. Les qualités personnelles sont celles qui leur permettent d'exécuter leur mandat de directeur autorisé de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit requis.

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

~~61.1.~~ ~~La politique de risque, qui met en œuvre la stratégie du conseil d'administration en matière de risques, comprend :~~

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

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

~~62.1. La politique en matière de fonds propres et de liquidités, qui met en œuvre la stratégie du conseil d'administration en matière de fonds propres et de liquidités réglementaires et internes, comprend en particulier :~~

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

## Chapitre 5. Organisation administrative, comptable et informatique

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

~~63-67.~~ 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. ~~Ces tâches de décision, d'exécution, comprenant l'initiation, l'enregistrement, le suivi et le contrôle des opérations, et de contrôle interne sont effectuées dans le cadre d'un organigramme des fonctions et d'une description des tâches arrêtés par la direction autorisée sous forme écrite. L'organigramme et la description des tâches sont~~ 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.

~~64-68.~~ L'organigramme retient pour les différentes fonctions (commerciales, de support ~~et~~ de contrôle) ainsi que pour les différentes unités opérationnelles (~~services, départements ou métiers~~) leur structure et les liens hiérarchiques et fonctionnels entre elles et avec la direction autorisée et ~~le conseil d'administration~~ l'organe de surveillance.

~~65-69.~~ La description des tâches à remplir par le personnel exécutant explique la fonction, les pouvoirs et la responsabilité de chaque exécutant.

~~66-70.~~ ~~Sans préjudice du point 72,~~ L'organigramme et la description des tâches sont établis sur base du principe de la séparation des tâches. En vertu de ce principe, les tâches et responsabilités doivent être attribuées de façon à éviter qu'elles ne soient incompatibles dans le chef d'une même personne. Le but poursuivi est d'écartier 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.

~~67-71.~~ Conformément ~~aux articles à l'article 7~~ ~~paragraphe 2 et 19,~~ paragraphe 2 de la LSF, la direction autorisée a une responsabilité collective en ce qui concerne la gestion de l'établissement. Le principe de la séparation des tâches ne ~~peut déroger~~ pas ~~déroger~~ à cette responsabilité conjointe. Cette dernière reste ~~d'ailleurs~~ compatible avec la pratique suivant laquelle les membres de la direction autorisée se répartissent les tâches journalières du suivi rapproché des différentes activités. ~~Dans ce contexte, la CSSF recommande d'organiser~~ L'établissement doit organiser cette répartition de manière à éviter les conflits d'intérêts. Ainsi, ~~il est recommandé de ne pas attribuer à~~ un même membre de la direction autorisée ~~les~~ 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~~ Par ailleurs, si dans un établissement de taille et d'activité limitées avec seulement deux directeurs agréés, il subsiste des conflits d'intérêt après l'attribution des fonctions de prises de risques et de contrôle entre ces deux directeurs et que ces conflits d'intérêt ne peuvent être mitigés de manière efficace, la nomination d'un troisième directeur autorisé, ~~qui assume lui-même le poste de « Chief Compliance Officer » suivant le point 141, ne peut pas en même temps être en charge de la fonction d'audit interne. Lorsque, en raison de la taille réduite de l'établissement, il est indispensable de regrouper plusieurs tâches et responsabilités sous une même personne, ce regroupement doit être organisé de sorte à ne pas porter préjudice à l'objectif poursuivi par la séparation des tâches.~~ est nécessaire.

~~68-72.~~ L'établissement dispose d'un programme de formation professionnelle continue qui assure que les membres du personnel ~~ainsi que le conseil d'administration~~ et ~~la~~ de l'organe de direction autorisée restent compétents et comprennent le dispositif de gouvernance interne ainsi que leurs propres rôles et responsabilités à cet égard.

~~69-73.~~ Chaque employé-membre du personnel doit prendre annuellement au moins dix-jours-consécutifs-deux semaines calendaires consécutives de congés personnels. Il doit être assuré que ~~l'employé~~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 5.32. La 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 en particulier un manuel des procédures clair, complet, détaillé et facilement accessible au-dont les procédures sont connues de l'ensemble du personnel de l'établissement concerné et qui est tenu à jour en continu.

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

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

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

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.

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

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 ainsi que les rapports de révision établis par le réviseur d'entreprises agréé sont conservés pendant cinq ans 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 L'autorité compétente 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.

Sous-chapitre 5.23. L'infrastructure administrative et technique

~~70-79.~~ L'établissement se dote des fonctions de support, des moyens matériels et techniques nécessaires et suffisants à l'exécution de ses activités.

#### **Section 5.23.1. L'infrastructure administrative des fonctions commerciales**

~~71-80.~~ 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 5.23.2. La fonction financière et comptable**

~~72-81.~~ 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~~ L'autorité compétente.

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

~~73-82.~~ 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<sup>74</sup>;
- d'expliquer l'évolution des soldes comptables d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables<sup>75</sup>;
- d'établir les comptes par application des règles de comptabilisation et d'évaluation définies par la législation comptable et la réglementation y afférente<sup>76</sup>;
- 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 l'autorité compétente<sup>77</sup>;
- de produire et de communiquer des informations périodiques à l'autorité compétente, 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<sup>78</sup>;
- de conserver toutes les pièces comptables suivant les dispositions légales en vigueur<sup>79</sup>;
- 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<sup>80</sup>;
- 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<sup>81</sup>;
- de s'assurer de la fiabilité du reporting financier.

74-83. 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.

75-84. Les tâches exercées au sein du service comptable et financier ne peuvent pas être cumulées avec d'autres tâches incompatibles, tant commerciales qu'administratives.

76-85. 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.

~~77-86.~~ 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.

~~78-87.~~ 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.

~~79-88.~~ 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 (~~point 12~~) afin d'éviter en particulier que le système comptable ne puisse être utilisé à des fins frauduleuses.

### **Section 5.~~23~~.3. La fonction informatique**

~~80-89.~~ 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 ~~point 12 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.

~~81-90.~~ Les établissements qui, en matière de fonction informatique, recourent aux services de tiers respectent en particulier les conditions définies à la section 7.4.2 au sous-chapitre 7.4 de cette partie.

**Section 5.23.4. Le dispositif de communication et d'alerte  
~~internes~~interne et externe**

~~82-91.~~ 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~~l'organe de direction, 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.

~~83-92.~~ 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 de l'organe de direction~~ 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 ~~importantes et~~ 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 de l'organe de surveillance~~. 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.

~~84-94.~~ 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 5.23.5. Le dispositif de gestion de crises**

~~85-95.~~ 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.

~~86-96.~~ Le dispositif de gestion de crises garantit qu'en situation de crise, les établissements de crédit fournissent au public les informations visées par les lignes directrices ~~de l'EBA publiées le 26 avril 2010 (« Principles for disclosures in times of stress (Lessons learnt from the financial crisis) »)~~. Ce point ne s'applique pas aux entreprises d'investissement du CEBS publiées le 26 avril 2010 (« Principles for disclosures in times of stress (Lessons learnt from the financial crisis) »).

97. Le dispositif de gestion de crises comprend un plan de redressement qui est conforme aux exigences du chapitre 2 de la partie IV de la LSF.

87-98. Le dispositif de gestion de crises fait l'objet de tests réguliers et de mises à jour en vue d'assurer et de maintenir son efficacité.

~~Sous-chapitre 5.3. — La documentation interne~~

~~88.1. — Les établissements documentent par écrit l'ensemble du dispositif en matière d'administration centrale et de gouvernance interne.~~

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

~~89.1. — La description des procédures pour l'exécution des activités (opérations) porte sur les points suivants :~~

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

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

~~90.1. — Les établissements documentent par écrit l'ensemble de leurs opérations, c'est-à-dire tout processus qui crée un engagement dans le chef de l'établissement ainsi que les décisions y relatives. La documentation doit être tenue à jour et conservée par l'établissement conformément à la loi. Elle doit être organisée de telle manière qu'elle puisse être aisément consultée par un tiers autorisé.~~

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

~~91.1. Les dossiers, documents de travail et rapports de contrôle des fonctions de contrôle interne, des experts et des sous-traitants visés au sous-chapitre 6.2 ainsi que les rapports de révision établis par le réviseur d'entreprises agréé sont conservés pendant cinq ans dans l'établissement luxembourgeois afin de permettre à l'établissement de retracer les contrôles effectués, les problèmes, déficiences ou irrégularités relevés ainsi que les recommandations et conclusions. La CSSF ainsi que le réviseur d'entreprises agréé doivent toujours pouvoir accéder à ces pièces.~~

~~92.1. Tous les ordres d'opérations initiés par l'établissement et toute la correspondance avec les clients ou leurs mandataires émanent de l'établissement ; toute la correspondance y est adressée. Au cas où l'établissement dispose d'une succursale à l'étranger, cette dernière constitue le point de contact pour sa propre clientèle.~~

## Chapitre 6. Le contrôle interne

~~93.99. Le contrôle interne est un dispositif composé de règles et de procédures qui ont pour but d'assurer de s'assurer que les objectifs posés par l'établissement sont atteints, que les ressources sont utilisées de façon économique et 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~~ l'autorité compétente sont respectées.<sup>10</sup>~~

~~94.100. 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.~~

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

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.

~~95. — Les trois lignes de défense sont complémentaires, chaque ligne de défense assumant ses responsabilités de contrôle indépendamment des autres lignes. Un environnement de contrôle interne solide nécessite la mise en place des contrôles suivants :~~

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

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.

#### 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***

~~96-101.~~ Les procédures en matière de contrôle interne prévoient que les exécutants contrôlent sur une base quotidienne les opérations qu'ils exécutent, ceci afin de détecter le plus rapidement possible des erreurs et omissions survenues dans le traitement des transactions courantes. On peut citer à titre d'exemples de tels contrôles, la vérification du solde de ~~la~~ caisse, la vérification de ses positions par le trader, le suivi de ses suspens par chaque ~~employé~~membre du personnel.

### **Section 6.1.2. Contrôles critiques continus**

~~97-102~~. Dans cette catégorie de contrôle tombent notamment :

- le contrôle hiérarchique~~7.1~~
- la validation (par exemple la double signature, les codes d'accès à des fonctionnalités données) associée au contrôle du respect de la procédure d'autorisation et de délégation de pouvoirs arrêtée par la direction autorisée (notamment en matière de crédits)~~7.1~~
- les contrôles réciproques~~7.1~~
- le relevé régulier de l'existence et de la valeur des éléments du patrimoine, notamment au moyen de la vérification des inventaires~~7.1~~
- la réconciliation et la confirmation des comptes~~7.1~~
- 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~~7.1~~
- le contrôle du respect des limites internes imposées par la direction autorisée (notamment en matière d'activités de marché et de crédits)~~7.1~~
- 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**

~~98-103~~. Les membres de la direction autorisée contrôlent personnellement et de manière régulière les activités et fonctions qui tombent sous leur responsabilité directe. Ces contrôles sont effectués sur base des données qui leur sont remises à cet effet par les fonctions commerciales, de support et de contrôle~~4~~ ou les différentes unités opérationnelles de l'établissement.

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

- les risques liés aux activités et fonctions dont ils sont directement responsables~~7.1~~
- le respect des lois et normes applicables à l'établissement, avec une attention particulière pour les normes prudentielles en matière de solvabilité, de liquidité, d'exposition de crédits non performants, de crédits restructurés et de la réglementation en matière de grands risques~~7.1~~
- le respect des politiques et procédures arrêtées par la direction autorisée conformément au point 18~~7.1~~
- le respect des budgets établis : examen des réalisations effectives et des écarts~~7.1~~
- le respect des limites (notamment sur base d'« exception reports »)~~7.1~~

- les caractéristiques des opérations, notamment leur prix, leur rentabilité individuelle ~~7~~ ;
- l'évolution de la rentabilité globale d'une activité.

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

#### Sous-chapitre 6.2. Les fonctions de contrôle interne

~~99-104.~~ Les politiques mises en œuvre en matière de contrôle des risques, de compliance et d'audit interne ~~conformément au point 18~~ instaurent trois fonctions de contrôle interne distinctes : d'une part, la fonction de contrôle des risques et la fonction compliance qui relèvent de la deuxième ligne de défense et, d'autre part, la fonction d'audit interne qui relève de la troisième ligne de défense ~~(voir point 9)~~. Ces politiques décrivent par ailleurs les domaines d'intervention relevant directement de chaque fonction de contrôle interne, règlent clairement les responsabilités en matière de domaines d'intervention communs 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.

~~100.~~ ~~Chaque fonction de contrôle interne est placée sous la responsabilité d'un chef de fonction distinct qui est nommé et révoqué suivant une procédure interne écrite. Lorsque, par application du principe de proportionnalité, un membre unique de la direction autorisée exerce les fonctions compliance et de contrôle des risques, cette personne cumule, par dérogation à ce qui précède, les postes de chef de la fonction compliance et de la fonction de contrôle des risques (voir aussi le point 72). Les nominations et révocations des responsables des fonctions de contrôle interne sont approuvées par le conseil d'administration et rapportées par écrit à la CSSF dans le respect de la procédure prudentielle d'approbation des titulaires de fonctions clé telle que publiée par la CSSF sur son site internet.~~

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

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

### **Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne**

~~101-105.~~ 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 conformément au point 116~~ qu'à l'organe de surveillance et, le cas échéant, aux comités spécialisés. Elles fournissent à la direction autorisée ainsi ~~qu'au conseil d'administration qu'à l'organe de surveillance et, le cas échéant, aux comités spécialisés~~ les avis et conseils qu'elles jugent utiles ~~en vue d'améliorer le dispositif d'administration centrale et de gouvernance interne de l'établissement ou qui leur sont demandés par ces organes ou comités~~.

~~102-106.~~ Les fonctions de contrôle interne répondent dans les meilleurs délais ~~aux demandes d'avis et de conseils émanant de la direction autorisée et du conseil d'administration ou des comités spécialisés le cas échéant. Lorsqu'elles~~ 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~~ l'organe de surveillance ou les comités spécialisés, le cas échéant, ~~suivant les modalités internes applicables~~.

~~103-107.~~ 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 ~~directions-organes de direction et conseils d'administration de surveillance~~ locaux ainsi qu'à la direction autorisée et ~~au conseil d'administration de l'établissement conformément au point 116~~ à l'organe de surveillance de tête de groupe.

### **Section 6.2.2. Caractéristiques des fonctions de contrôle interne**

~~104-108.~~ 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 à l'organe de surveillance~~ ou à son président, ou, le cas échéant, aux ~~présidents des~~ comités spécialisés qui en émanent, au réviseur d'entreprises agréé de l'établissement ainsi qu'à ~~la CSSF l'autorité compétente~~.

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

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

109. L'autorité dont doivent jouir les fonctions de contrôle interne requiert que ces fonctions puissent exercer leurs responsabilités de leur propre initiative, s'exprimer librement et accéder à toutes les données et informations externes et internes (dans l'ensemble des unités opérationnelles de l'établissement qu'elles contrôlent) qui sont jugées qu'elles jugent nécessaires pour l'accomplissement de leurs missions.

~~105-110.~~ Le personnel des Les fonctions de contrôle interne ou les tiers (~~voir point 110~~) agissant pour compte de ces fonctions doivent effectuer leurs travaux avec objectivité.

Afin de garantir leur objectivité, les personnes relevant de fonctions de contrôle interne possèdent l'indépendance d'esprit ~~et de jugement ; ils ; 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.

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

~~106-111.~~ Afin de garantir l'efficacité ~~Les membres~~ des fonctions de contrôle interne, ~~ses membres~~ doivent posséder à un niveau individuel et collectif des connaissances, des compétences et une expérience professionnelles élevées dans le domaine des activités bancaires et financières et ~~des plus particulièrement dans leur domaine de responsabilités en ce qui concerne les~~ normes applicables. ~~Cette compétence doit être évaluée en tenant compte non seulement~~ Conformément au principe de proportionnalité, le niveau de compétences requis augmente en fonction de l'organisation de l'établissement et de la nature ~~de la mission des collaborateurs, mais également, de l'échelle et de la complexité et de la diversité des activités exercées par l'établissement en vue de permettre une couverture intégrale~~ des activités et des risques. ~~Cette~~ 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 ~~les des~~ connaissances théoriques ~~qui leur permettent d'exercer cette fonction d'une manière efficace nécessaires.~~

~~107-112.~~ Pour garantir l'exécution des tâches qui leur incombent, les fonctions de contrôle interne disposent des ressources humaines, de l'infrastructure et des budgets nécessaires et suffisants, conformément au principe de proportionnalité ~~(point 4)~~. Le budget doit être suffisamment flexible pour tenir compte d'une adaptation des missions des fonctions de contrôle interne en réponse à des changements ~~du profil au niveau de~~ risque l'organisation, des activités et des risques de l'établissement. ~~Ces dispositions sont compatibles avec une sous-traitance ou en cas de la fonction d'audit interne et le recours des fonctions de contrôle interne à des experts externes conformément aux points 117 et 118.~~ survenance d'événements spécifiques.

~~108-113.~~ Le champ d'intervention des fonctions de contrôle interne couvre l'ensemble de l'établissement, dans le respect de leurs compétences respectives. Il inclut les activités inhabituelles et potentiellement non transparentes ~~visées à la section 7.1.1.~~

~~109-114.~~ Chaque établissement prend les mesures nécessaires pour assurer que les membres des fonctions de contrôle interne exercent leurs fonctions avec intégrité et discrétion.

### **Section 6.2.3. Exécution des travaux des fonctions de contrôle interne**

~~110-115.~~ Les fonctions de contrôle interne documentent les travaux effectués conformément aux responsabilités assignées, notamment afin de permettre de retracer les interventions ainsi que les conclusions retenues.

~~111.~~ 116. Les fonctions de contrôle interne rapportent par écrit régulièrement et si nécessaire sur base ad hoc à la direction autorisée et à l'organe de surveillance ou, le cas échéant, aux comités spécialisés. Ces rapports portent sur le suivi des recommandations, ~~des~~ problèmes, déficiences et irrégularités relevés par le passé ainsi que sur les nouveaux problèmes, déficiences et irrégularités identifiés. Chaque rapport spécifie les risques y liés ainsi que leur degré de gravité (mesure de l'impact) et propose des mesures correctrices, de même qu'en règle générale une prise de position des personnes concernées.

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

~~Conformément au point 107,~~ En cas de problèmes, déficiences et irrégularités graves, les responsables des fonctions de contrôle interne en informent immédiatement la direction autorisée, le président ~~du conseil d'administration de l'organe de surveillance~~ et les présidents des comités spécialisés, le cas échéant. Dans ces cas, ~~la CSSF recommande que~~ les responsables des fonctions de contrôle interne ~~soient~~ 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. Elles rapportent de manière régulière à ce sujet à la direction autorisée.

#### **Section 6.2.4. Organisation des fonctions de contrôle interne**

117. 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 l'organe de surveillance et rapportées par écrit à l'autorité compétente dans le respect de la Procédure prudentielle telle que publiée par la CSSF sur son site internet.

118. Les responsables des trois fonctions de contrôle interne sont responsables vis-à-vis de la direction autorisée et, en dernier ressort, vis-à-vis de l'organe de surveillance pour l'exécution de leur mandat. A ce titre, ces responsables doivent pouvoir contacter directement et de leur propre initiative le président de l'organe de surveillance 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.

119. 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 ~~soit~~ soient sous-traitées ~~danstraitées par~~ de petits établissements dont le profil de risques-risque est faible et non complexe, ~~moyennant le respect des conditions énoncées au point 118 et à la sous-section 6.2.7.4. Cette~~ Une telle sous-traitance n'est en principe pas acceptable dans le cas d'établissements qui ont des agences, des succursales ou des filiales.

L'organe de surveillance 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 un accès direct à l'organe de surveillance ou, le cas échéant, au président du comité d'audit.

120. Les dispositions du point ~~112~~ précédent n'excluent pas que les fonctions de contrôle interne aient recours à l'expertise ~~ou et~~ aux ~~moyens~~ 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~~ à l'organe de surveillance d'apprécier les dépendances et les risques qui résultent pour l'établissement d'un recours significatif à ces ~~tiersressources~~ ressources externes.

La direction autorisée sélectionne ces ~~tiers (« experts »)~~ ressources externes sur base d'une analyse d'adéquation entre les besoins de l'établissement et les services ~~et, le niveau d'objectivité et d'indépendance et les~~ compétences spécifiques offerts par ces tiers. ~~L'expert retenu doit, qui doivent~~ être indépendant indépendants du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent. L'organe de surveillance approuve les ressources externes sélectionnées par la direction autorisée.

121. Le Tout recours à ~~un expert externe des ressources externes doit se fait faire~~ sur base d'un mandat écrit. ~~L'expert réalise ses~~ Ces tiers réalisent leurs travaux dans le respect des dispositions réglementaires et internes ~~(notamment les chartes d'audit interne et de compliance)~~ qui sont applicables à la fonction de contrôle interne et au domaine de contrôle en question. ~~L'expert doit- Ils doivent~~ être placé placés sous la dépendance du responsable de la fonction de contrôle interne dont relève le domaine contrôlé. Ce responsable supervise les travaux de ~~l'expert ces~~ tiers.

~~115-122.~~ Conformément ~~Lorsqu'en application du principe de proportionnalité,~~ l'établissement peut démontrer qu'il n'est pas justifié de mettre en place une fonction distincte de contrôle des risques et une fonction compliance ou de nommer deux responsables à temps plein à la tête de ces deux fonctions, l'établissement peut mettre en place une fonction combinée ou un poste à responsabilité combinée, moyennant accord préalable de l'autorité compétente.

L'application du principe de proportionnalité ne peut cependant conduire au point 3, cumul d'autres responsabilités dans le chef d'une personne combinant déjà la responsabilité pour la fonction de contrôle des risques et la fonction compliance.

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, doit adresser une demande à l'autorité compétente qui comprendra :

- une description de la fonction combinée ou du poste à responsabilité combinée,
- l'analyse et ses conclusions justifiant la création d'une fonction combinée ou d'un poste à responsabilité combinée au vu de l'organisation de l'établissement, de la nature, de l'échelle et de la complexité de ses activités et risques, et
- la décision de l'organe de surveillance approuvant l'analyse et ses conclusions.

123. L'établissement qui, en application du principe de proportionnalité, désire soustraire les tâches opérationnelles de la fonction d'audit interne doit adresser une demande préalable à l'autorité compétente qui comprendra :

- 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, ainsi que
- la personne responsable de cette sous-traitance au sein de l'établissement,
- l'analyse et ses conclusions justifiant la sous-traitance des tâches opérationnelles de la fonction d'audit interne, et
- la décision de l'organe de surveillance approuvant l'analyse et ses conclusions et, le cas échéant, l'avis du comité d'audit.

Ces prestataires externes peuvent être les auditeurs internes du groupe dont fait partie l'établissement. Il appartient à l'organe de surveillance 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.

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

~~116-125.~~ Dans ~~Pour~~ les succursales ~~de l'établissement,~~ les fonctions de contrôle interne dépendent, d'un point de vue hiérarchique et fonctionnel, des fonctions de contrôle ~~de l'établissement tête de groupe 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 ~~l'établissement tête de groupe dont elles font partie.~~ la tête de groupe. Les responsables des fonctions de contrôle de la tête de groupe doivent donner leur accord pour tout recrutement, licenciement et décisions importantes sur la rémunération des chefs des fonctions de contrôle des succursales et/ou filiales. Les rapports établis conformément aux dispositions de la présente circulaire sont soumis non seulement ~~aux organes de~~ à la direction et à l'organe de surveillance ~~locaux local,~~ mais également, en synthèse, aux fonctions de contrôle interne de ~~l'établissement~~ la tête de groupe qui les analyse et qui fait rapport des points à relever, conformément au point 116.

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 annuels sur place, auprès de ces entités.

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

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

~~117.126.~~ Les principes de la présente circulaire n'excluent pas que, pour des établissements luxembourgeois qui sont succursale ou filiale de professionnels financiers luxembourgeois ou non, disposant de fonctions de contrôle interne au niveau de ces professionnels, les fonctions de contrôle interne soient liées de façon fonctionnelle à celles du professionnel en question.

#### **Section 6.2.5. La fonction de contrôle des risques**

##### **Remarques:**

~~1. Le lecteur est prié de se référer aussi aux points 9, 17, 21, 33, 45 à 51, 57, 104 à 121, 147 et 179 qui concernent également la fonction de contrôle des risques.~~

~~2. Le terme fonction de *contrôle* des risques est emprunté aux lignes directrices de l'EBA (« EBA Guidelines on Internal Governance (GL 44) ». Cette terminologie n'entend pas réduire cette fonction à un simple « contrôle » ex post de limites en risque tel que visé à la deuxième phrase du point 124. La fonction de contrôle des risques assume plus largement des tâches d'analyse et de suivi des risques conformément au point 123.~~

~~3. La fonction de contrôle des risques soumet son rapport annuel de synthèse en copie à la CSSF (points 116 et 210). Conformément au point 116, ce rapport contient un état des lieux en matière de risques et fait ainsi double emploi potentiel avec le rapport ICAAP (point 61) que la direction autorisée prépare à l'attention du conseil d'administration. Le risque de redondances existe d'autant plus que généralement la fonction de contrôle des risques est associée à la rédaction du rapport ICAAP. Afin d'éviter tout double emploi indu entre le rapport ICAAP et le rapport de synthèse de la fonction de contrôle des risques, il suffit que pour l'évaluation du risque suivant l'optique de l'ICAAP, la fonction de contrôle des risques réfère dans son rapport de synthèse au rapport ICAAP pour autant qu'elle partage les descriptifs et analyses de risques qui y figurent. Lorsqu'elle procède de la sorte, la fonction de contrôle des risques doit néanmoins émettre dans son rapport de synthèse ses propres conclusions qu'elle tire des descriptifs et analyses précitées. Le rapport de synthèse porte alors uniquement sur les autres domaines visés au point 116. Par contre, lorsque la fonction de contrôle des risques ne partage pas les descriptifs et analyses précitées, elle en fera mention explicite dans son rapport de synthèse où elle fait figurer ses propres évaluations.~~

~~4. Un autre domaine de redondances potentielles existe au niveau du partage des tâches entre la fonction compliance, responsable pour les risques de conformité (point 131), et la fonction de contrôle des risques, responsable pour « l'ensemble des risques » (point 123). Les établissements veillent à ce que l'allocation de ces tâches soit organisée en interne d'une manière efficace et efficiente.~~

~~118. La fonction de contrôle des risques est confiée à un service dédié composé d'une ou de plusieurs personnes.~~

~~119. La fonction de contrôle des risques est responsable pour l'anticipation, la détection, la mesure, le suivi, le contrôle et la déclaration de l'ensemble des risques auxquels l'établissement est ou pourrait être exposé et ainsi d'assister la direction autorisée dans la maîtrise des risques. Elle veille à ce que les risques soient adéquatement gérés.~~

~~Ces tâches sont à réaliser continuellement et sans délais.~~

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

127. 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 l'organe de surveillance 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 de l'organe de surveillance. Le terme fonction de contrôle des risques n'entend donc pas réduire cette fonction à un simple « contrôle » ex-post de limites.

128. Le champ d'intervention de la fonction de contrôle des risques comprend également 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.

129. La fonction de contrôle des risques veille à ce que les objectifs et limites réglementaires et 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 de ces limites, surveille la bonne application, propose des mesures de remédiation appropriées en cas d'infraction, veille au respect de la procédure d'escalade prévue en cas de dépassement d'infraction matérielle et veille à ce s'assure que les dépassements soient régularisés dans les meilleurs délais.

~~121-~~130. Le responsable de la fonction de contrôle des risques veille à ce que la direction autorisée et ~~le conseil d'administration l'organe de surveillance~~ reçoivent une vue indépendante, complète, objective et pertinente des risques auxquels l'établissement est ou pourrait être exposé<sup>11</sup>. Cette vue comprend en particulier une évaluation de l'adéquation entre ces risques et les fonds propres, ~~les (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 ~~les stratégies fixées par le conseil d'administration, en particulier en matière de tolérance à l'égard du risque, l'appétit au risque défini par l'organe de surveillance.~~ 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 l'autorité compétente, 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.

~~122-~~131. 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.

~~123-~~132. La fonction de contrôle des risques veille à ce que l'appréciation ~~qualitative et quantitative~~ des risques se fonde sur des hypothèses prudentes et sur un éventail de scénarios pertinents, en particulier en ce qui concerne les dépendances entre risques. Les appréciations quantitatives sont à valider par des méthodes d'appréciation qualitatives et des jugements (d'experts) qualitatifs, basés sur des analyses structurées et documentées.

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

<sup>11</sup> Dans le respect des « Principles for effective risk data aggregation and risk reporting » (BCBS 239) de janvier 2013

~~124-133.~~ 133. 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*

~~125.~~ 125. Lorsque, en vertu du principe de proportionnalité (point 4), la création d'un poste de « Chief Risk Officer » à plein temps n'est pas nécessaire, il est admissible d'en charger une personne à temps partiel.

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

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

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

134. 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.

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 à l'organe de surveillance.

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**

#### **Remarques:**

1. Le lecteur est prié de se référer aussi aux points 9, 17, 21, 33, 44, 55, 57, 104 à 121, 147 et 179 qui concernent également la fonction compliance.

2. Un domaine de redondances potentielles existe au niveau du partage des tâches entre la fonction compliance, responsable pour les risques de conformité (point 131), et la fonction de contrôle des risques, responsable pour « l'ensemble des risques » (point 123). Les établissements veillent à ce que l'allocation de ces tâches soit organisée en interne d'une manière efficace et efficiente.

~~126. La fonction compliance est confiée à un service dédié composé d'une ou de plusieurs personnes.~~

~~127. La fonction compliance a pour objectif d'anticiper, de détecter et d'évaluer les risques de compliance d'un établissement ainsi que d'assister la direction autorisée dans la maîtrise de ces risques. Ces derniers peuvent comporter une variété de risques tels que le risque de réputation, le risque légal, le risque de contentieux, le risque de sanctions ainsi que certains aspects du risque opérationnel, ceci en relation avec l'intégralité des activités de l'établissement.~~

~~Cette tâche est à réaliser continuellement et sans délais.~~

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

#### **Précision:**

La présente circulaire comprend les « orientations générales » contenues dans ~~le document ESMA/2012/388~~ les orientations de l'ESMA concernant certains aspects de la directive MIF 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 ~~le document~~ les orientations ESMA/2012/388.

*Sous-section 6.2.6.1. La charte de compliance*

~~128-137.~~ 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~~ l'organe de surveillance en dernier ressort.

~~129-138.~~ 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 de l'organe de surveillance ou, le cas échéant, les membres du comité d'audit ou du comité de compliance, ainsi que ~~la CSSF~~ l'autorité compétente.

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

~~130-~~139. \_\_\_\_\_ La charte de compliance doit être mise à jour dans les meilleurs délais pour tenir compte de changements au niveau des normes en vigueur 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~~ l'organe de surveillance 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 ~~et champ d'application~~ de la fonction compliance*

~~131-~~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.

~~132-~~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 ses-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. ~~Dans l'élaboration de ces règles, la fonction compliance tient compte, pour autant que de besoin pour l'établissement en question, des règles de déontologie énoncées dans le dispositif de la gouvernance interne, 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, ~~l'intégrité des marchés d'instruments financiers~~ les fraudes, la protection des intérêts et des données des clients et ~~des investisseurs, la protection des données et le respect du secret professionnel~~, la prévention et la gestion des conflits d'intérêts, ~~la prévention de l'utilisation du secteur financier par des tiers pour contourner leurs obligations réglementaires et la gestion du risque de conformité lié aux activités transfrontalières. Dans le cadre plus général du respect du code de conduite, la fonction compliance est aussi amenée à couvrir des domaines d'éthique et de déontologie, voire de fraudes.~~ Cette liste n'est pas exhaustive ~~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 l'autorité compétente 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 ~~telle manière qu'elle couvre façon à couvrir~~ tous les domaines pouvant donner lieu à des risques de compliance. ~~Toutefois, dans la mesure où dans la pratique certains domaines donnant lieu à des risques de compliance peuvent aussi relever d'autres fonctions telles que la fonction de contrôle des risques, la fonction finance ou la fonction juridique, et dans un souci d'éviter une duplication des contrôles de compliance,~~ Il est admissible que les domaines autres que ceux énumérés ci-dessus ne soient pas directement couverts par la fonction compliance. ~~Il est entendu que dans ce cas,~~ Le risque de compliance est alors à couvrir par les autres fonctions de contrôle interne suivant une politique de compliance définissant clairement les attributions et les responsabilités des différents intervenants en la matière et moyennant le respect de la ségrégation des tâches. Dans ce cas, le « Chief Compliance Officer » assume un rôle de coordination, de centralisation de l'information et de vérification que les autres domaines ne relevant pas directement de son champ d'intervention sont bien couverts.
- ~~Il appartient à l'établissement de décider si, compte tenu des particularités des activités exercées, sa fonction compliance couvre le contrôle du respect des règles n'ayant pas directement trait aux activités bancaires et financières à proprement parler, telles que notamment les règles relevant du droit de travail, du droit social, du droit des sociétés ou du droit de l'environnement.~~

~~133-142.~~ 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.

~~134-143.~~ 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 de l'organe de surveillance) ou externes (par exemple rapports du réviseur externe d'entreprises agréé, correspondance de la part de l'autorité de contrôle).

~~135-144.~~ 144. La fonction compliance assiste et conseille la direction autorisée pour des questions de compliance et de normes, 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.

~~136-145.~~ 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.

~~137-146.~~ 146. Le « Chief Compliance Officer » est la personne de contact privilegié 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*

~~138. — Lorsque, en vertu~~ Les établissements créent une fonction compliance permanente et indépendante compte tenu du principe de proportionnalité (point 4), ~~la création d'un poste de « Chief Compliance Officer » à plein temps n'est pas nécessaire, il est admissible d'en charger une personne à temps partiel.~~

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

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

~~Il est admissible, moyennant autorisation spécifique de la CSSF, que le membre de la direction autorisée désigné comme étant directement en charge de la fonction compliance assume lui-même le poste de « Chief Compliance Officer ».~~ considérations générales sur l'organisation des fonctions de contrôle interne élaborées à la section 6.2.4.

#### **Section 6.2.7. La fonction d'audit interne**

~~139. La fonction d'audit interne est confiée à un service d'audit interne, composé d'une ou de plusieurs personnes.~~

~~140. La fonction d'audit constitue à l'intérieur de l'organisation de l'établissement une fonction indépendante et permanente d'évaluation critique de l'adéquation et de l'efficacité de l'administration centrale, de la gouvernance interne et de la gestion des activités et des risques dans leur intégralité afin d'assister le conseil d'administration et la direction autorisée de l'établissement et leur permettre d'avoir la meilleure maîtrise de leurs activités et des risques y liés et ainsi de protéger son organisation et sa réputation.~~

*Sous-section 6.2.7.1. La charte d'audit interne*

~~141.147.~~ 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, l'organe de surveillance~~.

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 ~~élé~~ clés (indépendance, objectivité, intégrité, compétence, autorité, suffisance des ressources) ~~7.1~~
- conférer à la fonction d'audit interne le droit d'initiative et l'autoriser à examiner toutes les activités et fonctions de l'établissement ~~7.1~~ y compris celles de ~~leurs ses~~ succursales ~~à l'étranger~~ 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 ~~dans~~ pour l'établissement, dans la mesure requise pour l'exercice de sa mission ~~7.1~~
- définir les lignes de communication hiérarchiques et fonctionnelles des conclusions qui se dégagent des missions d'audit ~~7.1~~
- définir les relations avec les fonctions compliance et de contrôle des risques ~~7.1~~
- définir les conditions et circonstances applicables lorsqu'il est fait recours à l'expertise de tiers ~~7.1~~
- 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 ~~7.1~~
- définir les responsabilités et lignes de reporting du responsable de la fonction d'audit interne ~~7.1~~
- établir le droit pour le « Chief Internal Auditor » de contacter directement et de sa propre initiative le président ~~du conseil d'administration de l'organe de surveillance~~ ou, le cas échéant, les membres du comité d'audit ainsi que ~~la~~ CSSF, l'autorité compétente ;

- préciser ~~que les missions d'audit interne sont effectuées en conformité avec des standards professionnels reconnus~~ qui gouvernent le fonctionnement et les travaux de l'audit interne<sup>12</sup> ;
- préciser les procédures à respecter en matière de coordination et de coopération avec le réviseur d'entreprises agréé.

Le contenu de la charte d'audit interne est porté à la connaissance de tous les membres du personnel de l'établissement, y compris ceux qui travaillent dans les succursales ~~à l'étranger et dans les~~ 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~~ l'organe de surveillance en dernier ressort. Elles sont portées à la connaissance de tous les membres du personnel.

~~142-148.~~ En complément des points 110 à 112, Le service d'audit interne est suffisant en nombre et dispose de compétences suffisantes dans son ensemble pour couvrir toutes les activités de l'établissement. Les auditeurs internes doivent avoir des connaissances suffisantes des techniques d'audit.

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

<sup>12</sup> tels que par exemple l'« International Professional Practices Framework (IPPF) » de l'Institute of Internal Auditors (IIA)

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

~~143-149.~~ D'une manière générale, La fonction d'audit interne examine et évalue si le dispositif, entre autres (liste non exhaustive<sup>13</sup>), en matière d'administration centrale fonction de l'organisation et de gouvernance interne est adéquat à la nature, de l'échelle et fonctionne de manière efficace. A ce titre, de la fonction d'audit interne évalue, entre autres complexité des activités :

- le suivi du respect des lois et réglementations ainsi que des exigences prudentielles imposées par ~~la CSSF, l'autorité compétente ;~~
- 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 à l'organe de surveillance~~ et aux comités spécialisés, le cas échéant, à la direction autorisée et à ~~la CSSF, l'autorité compétente ;~~
- ~~l'exécution des décisions prises par la direction autorisée et par les personnes agissant par voie de délégation et sous sa responsabilité,~~
- le respect des politiques et procédures, en particulier celles régissant l'adéquation des fonds propres et des réserves de ~~liquidité liquidités~~ internes en application ;
- L'intégrité des processus devant assurer la fiabilité des points 67 deuxième méthodes et outils utilisés par l'établissement, les hypothèses et troisième tirets données utilisées dans les modèles internes, les outils qualitatifs servant à l'identification et 125, l'évaluation des risques ainsi que les mesures d'atténuation du risque qui sont prises.
- ~~l'adéquation de la gestion des risques,~~
- ~~le fonctionnement et l'efficacité des fonctions compliance et de contrôle des risques (sections 6.2.5 et 6.2.6).~~

<sup>13</sup> 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.

~~144-150.~~ \_\_\_\_\_ 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.

~~145-151.~~ \_\_\_\_\_ ~~En complément des points 119 et 120,~~ La mise en place d'une fonction d'audit interne ~~local~~ 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 ~~locaux~~ locales.

~~146.~~ Le « Chief Internal Auditor » ~~doit s'assurer que le service applique les normes internationales de l'Institute of Internal Auditors ou des normes internationales équivalentes en application du point 21 ainsi que les règles de conduite en application du point 55.~~

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

~~147-152.~~ \_\_\_\_\_ L'ensemble des missions d'audit interne est planifié et exécuté selon un «plan d'audit interne». Le plan est établi par le responsable de la fonction d'audit interne pour une période pluriannuelle (en principe trois ans) avec comme objectif de couvrir l'ensemble des activités et des fonctions, en tenant compte à la fois des risques que présentent une activité ou une fonction ~~de l'établissement~~ et de l'efficacité de l'organisation et du contrôle interne en vigueur pour cette activité ou fonction (approche basée sur le risque). Le plan tient compte des avis ~~du conseil d'administration et de l'organe de surveillance 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 l'autorité compétente~~) et tient compte également des développements et innovations prévus ainsi que des risques qui peuvent en découler.

~~149-153.~~ Le plan est discuté avec la direction autorisée et ~~soumis à la direction autorisée et approuvé par elle, confirmé par~~ le comité d'audit, le cas échéant, et approuvé en dernier ressort par ~~le conseil d'administration, l'organe de surveillance~~. Il est à revoir sur une base annuelle et à adapter ~~le cas échéant~~ en fonction des développements et des urgences. Toute adaptation est à ~~approuver formellement revoir~~ par la direction autorisée et le comité d'audit, le cas échéant, ~~avant d'être approuvée par l'organe de surveillance~~. L'approbation implique que la direction autorisée mette à la disposition du service d'audit interne les moyens nécessaires pour l'exécution du plan d'audit interne.

Dans son rapport de synthèse ~~au conseil d'administration suivant le point 116 à l'organe de surveillance~~, 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 l'organe de surveillance~~ : missions annulées, missions reportées ainsi que missions dont le champ d'application a été changé de manière significative.

~~149-154.~~ Le plan ~~qui est suffisamment documenté,~~ définit les objectifs de chaque mission et l'étendue des travaux à réaliser, estime le temps et les ressources humaines et matérielles nécessaires et attribue à chaque activité et risque une fréquence d'audit.

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

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.

~~150-155.~~ Dans l'hypothèse où le service d'audit interne de la maison mère de l'établissement luxembourgeois procède régulièrement à des contrôles sur place auprès de sa filiale, il ~~se recommande 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.

~~151-156.~~ 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.

~~152-157.~~ 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.

~~153-158.~~        Chaque mission doit faire l'objet d'un rapport écrit du service d'audit interne destiné, en règle générale, aux personnes contrôlées, à la direction autorisée ainsi que - éventuellement sous forme de synthèse - ~~au conseil d'administration à l'organe de surveillance~~ (et au comité d'audit, le cas échéant) ~~suivant le point 116~~. Les rapports sont également à tenir à disposition du réviseur d'entreprises agréé et de ~~la CSSF, l'autorité compétente~~. Ces rapports sont à rédiger en français, allemand ou anglais.

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

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

~~154.~~ ~~L'établissement qui conformément au point 117 décide de sous-traiter la fonction d'audit interne, doit introduire une demande écrite auprès de la CSSF. Cette demande comprend les informations nécessaires à son appréciation, dont notamment le nom de l'expert externe, personne physique, qui assumera la fonction d'audit interne de l'établissement.~~

~~159.~~ ~~Le choix de l'expert externe qui réalise les travaux d'audit interne doit être approuvé par le conseil d'administration, le cas échéant sur base de l'avis du comité d'audit créé par application du point 33. L'expert retenu doit être indépendant du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent. Il réalise ses travaux conformément au point 118 et, mutatis mutandis, aux dispositions contenues dans la présente circulaire. A ce titre, il s'acquitte de l'ensemble~~ 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.

~~— En cas de sous-traitance des tâches et responsabilités que la présente circulaire donne à opérationnelles de l'audit interne-~~

~~155-160.~~        ~~En cas de recours à un expert externe pour certains aspects conformément au point 118, cet expert réalise ses, 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 ~~ses-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 ~~« Chief Internal Auditor »~~ responsable désigné de la fonction, à la direction autorisée, au comité d'audit, le cas échéant, et ~~au conseil d'administration suivant le point 116 à l'organe de surveillance~~.

~~156. Les experts externes suivant le point 118 peuvent être les auditeurs internes du groupe dont fait partie l'établissement. Lorsque les experts exercent la profession de réviseur d'entreprises agréé, ils doivent à tous égards être indépendants du réviseur d'entreprises et du cabinet de révision agréés de l'établissement ainsi que du groupe dont ces personnes relèvent.~~

## Chapitre 7. Exigences spécifiques

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

~~157-161.~~ 161. La structure organisationnelle, en termes d'entités (structures) juridiques, est appropriée et justifiée par rapport aux stratégies et principes directeurs ~~visés au point 17 de la présente circulaire.~~ Elle est claire et transparente aux yeux de l'ensemble des parties prenantes.

~~Elle~~ La structure juridique, organisationnelle et opérationnelle doit permettre et promouvoir une gestion efficace, saine et prudente des activités. Elle ne doit pas entraver la capacité bonne gouvernance de l'établissement, en particulier ~~de ses organes d'administration et~~ 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.

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

~~158-162.~~ 162. Les principes directeurs que ~~le conseil d'administration l'organe de surveillance~~ 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 l'organe de surveillance, à la direction autorisée, aux fonctions de contrôle interne ou à ~~la CSSF l'autorité compétente~~, à leur demande.

**Section 7.1.1. ~~Principes directeurs en matière d'activités~~  
~~«Structures complexes et activités inhabituelles» ou~~  
~~«potentiellement non transparentes»~~**

~~159-163.~~ Les activités ~~«inhabituelles»~~ ou ~~«potentiellement non transparentes»~~ sont celles des activités qui sont réalisées à travers des entités ~~(structures) ou montages~~ juridiques ~~dédiées ou assimilées («special purpose vehicles»)~~ complexes ou dans des territoires qui accusent des déficits en matière de transparence ou qui ne répondent pas aux normes bancaires internationales.

~~160.~~ Les principes directeurs que ~~le conseil d'administration l'organe de surveillance~~ arrête en matière de gouvernance interne prévoient en particulier que les structures complexes et les activités inhabituelles ou potentiellement non transparentes

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

~~161-164.~~ Les points ~~162 et 163~~ s'appliquent aussi lorsque l'établissement mène ~~des activités inhabituelles ou non transparentes~~ particulier ceux liés à la criminalité financière. Ou'il s'agisse d'activités pour le compte propre ou pour compte de ses 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

~~162-165.~~ La politique en matière de gestion des conflits d'intérêts couvre l'ensemble des conflits d'intérêts, ~~avec pour des raisons économiques, personnelles, professionnelles ou politiques, qu'ils soient persistants ou liés à un événement unique.~~ Une attention particulière ~~pour les 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 ~~les aux~~ membres du conseil d'administration de l'organe de surveillance.

~~163-166.~~ La politique en matière de gestion des conflits d'intérêts prévoit que tous les conflits d'intérêts actuels et potentiels doivent être détectés, ~~avec pour objectif de les éviter~~ 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 ~~dans l'intérêt de de façon à éviter que~~ l'établissement, ses contreparties et ~~conformément aux dispositions réglementaires applicables en matière de protection des les clients-~~ n'en subissent les conséquences injustifiées. La politique et les procédures en question fixe comprennent également la procédure à suivre en cas de non-respect de la politique en question.

~~167.~~ La politique en matière de gestion des conflits d'intérêts ~~identifie les 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 est ou pourrait son personnel et ses représentants sont ou pourraient~~ être ~~confronté~~ 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 ~~ces conflits d'intérêts~~ ils doivent être gérés.

~~164-168.~~ Afin de minimiser le potentiel de conflits d'intérêts, l'établissement met en place une ségrégation appropriée des tâches et ~~activités-~~ 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 »).

~~165-169.~~ La politique en question 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. ~~Ce dernier, lorsqu'il constate que le conflit d'intérêt est acceptable au vu de la politique interne, l'autorise suivant les modalités et conditions prévues par cette politique. La politique en question fixe également la procédure d'escalade qui détermine les conflits d'intérêts qui doivent être rapportés à la direction autorisée et autorisés par celle-ci.~~

Les membres de la direction autorisée et ~~du conseil d'administration de l'organe de surveillance~~ qui sont sujets à un conflit d'intérêts en informent respectivement la direction autorisée ou ~~le conseil d'administration l'organe de surveillance~~ 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.<sup>14</sup>

~~166-170.~~ La détection et la gestion des conflits d'intérêts appartiennent au champ d'intervention des fonctions de contrôle interne.

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

~~167-171.~~ Les ~~relations d'affaires-opérations~~ avec des parties liées sont soumises pour approbation ~~au conseil d'administration à l'organe de surveillance~~ lorsqu'elles ont ou pourraient avoir, ~~individuellement ou de manière agrégée~~, une influence significative et défavorable sur le profil de risque de l'établissement. ~~La règle s'applique également lorsqu'en l'absence d'effet significatif au niveau de chaque transaction prise individuellement, l'influence est significative pour l'ensemble des transactions avec des parties liées.~~

~~168-172.~~ Tout changement matériel relatif à des transactions significatives effectuées avec des parties liées doit être porté à l'attention ~~du conseil d'administration de l'organe de surveillance~~ dans les meilleurs délais.

~~169-173.~~ Les transactions avec des parties liées doivent être réalisées dans l'intérêt de l'établissement. L'intérêt de l'établissement n'est pas respecté lorsqu'il s'agit en particulier de transactions avec des parties liées qui :

- sont réalisées à des conditions moins avantageuses ~~(dans le chef de l'établissement)~~ que celles qui s'appliqueraient à la même transaction réalisée avec une partie tierce (« at arm's length »), ~~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 ;

<sup>14</sup> 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.

- sont contraires aux principes d'une gestion saine et prudente dans l'intérêt de l'établissement.

~~170-174.~~ \_\_\_\_\_ Lorsqu'il est tête de groupe, l'établissement veille à prendre en compte d'une manière équilibrée et dans le respect des dispositions légales applicables, les intérêts de toutes les entités juridiques et succursales qui composent le groupe. Ces intérêts sont à apprécier à la lumière de leur contribution aux objectifs et intérêts communs du groupe à long terme.

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

~~171.~~ On entend par « nouveaux produits » toute modification de l'activité ~~(en termes de couverture de marchés et de clientèle, de produits et de services)~~.

~~172.~~ Aucune nouvelle activité ne doit être entreprise avant que l'approbation n'ait été donnée par la direction autorisée, après avoir entendu toutes les parties concernées, et que les moyens mentionnés au point 179 ne soient disponibles. Le processus en question est fixé dans une procédure d'approbation des nouveaux produits qui respecte les dispositions des points 177 à 180.

~~173-175.~~ \_\_\_\_\_ 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 l'organe de surveillance, avec la stratégie en matière de risque, l'appétit pour le risque de l'établissement et les limites correspondantes.

~~174-176.~~ \_\_\_\_\_ La procédure d'approbation des nouveaux produits définit en particulier les modifications d'activités sujettes à la procédure d'approbation ~~(modification d'activité dite significative)~~, 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.

~~175.~~ La procédure d'approbation fixe les droits et obligations de toutes les parties concernées, y compris les fonctions de contrôle interne, ainsi que les conditions à remplir en vue d'une approbation. Ces conditions incluent la compliance, la maîtrise des calculs de valorisation (« pricing ») et des risques, l'expertise interne, l'infrastructure technique et les ressources humaines suffisantes pour assurer l'ensemble du traitement opérationnel.

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.

177. 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. ~~Pour leurs avis, les fonctions de contrôle interne peuvent s'appuyer sur les analyses faites par les unités opérationnelles.~~

~~176-178. 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.~~

~~177-179.~~ Les fonctions de contrôle interne peuvent exiger qu'une modification d'activités soit classée comme significative-matérielle et soumise par conséquent à la procédure d'approbation.

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

~~178-180.~~ 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.

~~Lorsqu'une sous-traitance de nature informatique, ou une chaîne de sous-traitance composée exclusivement de sous-traitances de nature informatique, repose sur une infrastructure de cloud computing telle que définie dans la circulaire 17/654, les points du sous-chapitre 7.4 de la présente circulaire ne s'appliquent pas et il convient au professionnel financier de respecter les exigences de la circulaire 17/654.~~

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.

181. 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**

~~179-182.~~ La sous-traitance ne doit pas aboutir à ce que les règles de la présente circulaire en matière d'administration centrale (~~chapitres 1 et 3~~) ne soient plus respectées.

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

- Les fonctions stratégiques ou relevant du cœur de métier ne peuvent pas être sous-traitées ;
- L'établissement conserve l'expertise nécessaire pour contrôler efficacement les prestations ou les tâches sous-traitées et la gestion des risques associés à la sous-traitance ;
- ~~• La protection des données doit être garantie en permanence ;~~
- ~~• 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, ~~sauf concernant la responsabilité du secret professionnel lorsque le sous-traitant agit dans le cadre de l'article 41(5) de la LSF ;~~
- La responsabilité finale de la gestion des risques associés à la sous-traitance incombe à ~~la direction autorisée de~~ l'établissement procédant à la sous-traitance ;
- ~~• L'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles.~~

- 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 l'autorité compétente. Une notification à ~~la~~ CSSF l'autorité compétente, 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 l'autorité compétente, du réviseur d'entreprises agréé et des fonctions de contrôle interne de l'établissement aux informations relatives aux activités sous-traitées doit être garanti en vue de leur permettre d'émettre une opinion fondée sur l'adéquation de la sous-traitance. Cet accès inclut que les précités peuvent également vérifier les données pertinentes détenues par un partenaire externe et, dans les cas ~~prévues~~ 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.

~~180-183.~~ 183. L'établissement qui sous-traite appuie sa décision de sous-traiter sur une analyse préalable et approfondie, démontrant qu'elle n'entraîne pas de délocalisation de l'administration centrale. Celle-ci portera au moins sur une description circonstanciée des services ou activités à sous-traiter, sur les effets attendus de la sous-traitance ainsi que sur une évaluation approfondie des risques du projet de sous-traitance envisagé sur le plan des risques financiers, opérationnels, légaux et de réputation. L'analyse comprendra une évaluation détaillée (due diligence) du prestataire de services proposé.

~~181-184.~~ 184. Une attention particulière doit être portée à la sous-traitance d'activités critiques au niveau desquelles la survenance d'un problème pourrait avoir un effet significatif sur la capacité de l'établissement à respecter les exigences réglementaires, voire à poursuivre son activité.

~~182-185.~~ 185. Une attention particulière doit être accordée aux risques de concentration et de dépendance qui apparaissent lorsque de larges parties d'activités ou de fonctions importantes sont sous-traitées à un prestataire unique pendant une période prolongée.

~~183-186.~~ Les établissements doivent prendre en compte les risques associés aux «chaînes» de sous-traitance (lorsqu'un prestataire sous-traite une partie des activités sous-traitées à d'autres prestataires). A cet égard, ils accordent une attention particulière à la sauvegarde de l'intégrité du contrôle interne et externe. En outre, l'établissement veillera à fournir à ~~la CSSF~~ l'autorité compétente tous les éléments permettant de montrer que le processus de sous-traitance en cascade est maîtrisé.

~~184-187.~~ La politique en matière de sous-traitance tient compte de l'impact de la sous-traitance sur les activités et les risques de l'établissement ~~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 ~~de 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~~ l'autorité compétente ou ~~d'entraver~~ d'entraver la surveillance ~~par la CSSF~~.

~~185-188.~~ 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'événements 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 ~~fournisseur 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.

~~186-189.~~ Pour chaque activité sous-traitée, l'établissement désignera parmi ~~ses employés 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**

~~187-190.~~ 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.

~~188-191.~~ La politique de l'établissement en matière de sécurité des systèmes d'information prend en compte la sécurité individuelle mise en place par son ou ses sous-traitants, afin de s'assurer notamment de la cohérence de l'ensemble.

~~189-192.~~ La sous-traitance en matière informatique peut porter sur des services de conseil, de développement et de maintenance (sous-section 7.4.2.2), des services d'hébergement (sous-section 7.4.2.3) ou des services de gestion/d'opération des systèmes informatiques (sous-section 7.4.2.1).

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

~~190-193.~~ Les établissements peuvent recourir contractuellement à des services de gestion/d'opération de leurs systèmes :

- Au Luxembourg, uniquement auprès :
- d'un établissement de crédit ou d'un professionnel financier disposant d'un agrément de PSF de support selon les articles 29-3 et 29-4 de la LSF (statut d'opérateurs de systèmes informatiques primaires du secteur financier ou statut d'opérateurs de systèmes informatiques secondaires et de réseaux de communication du secteur financier) ;
- d'une entité du groupe auquel l'établissement appartient et qui traite exclusivement des opérations de groupe, ~~à condition que. Au cas où~~ ces systèmes ~~ne contiennent aucune donnée confidentielle lisible des données confidentielles lisibles~~ concernant les clients. ~~Dans le cas contraire, l'établissement s'assure, veille au regard des éventuels risques juridiques et obligations légales, respect des dispositions de l'article 41, paragraphe 2bis de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles LSF.~~
- A l'étranger, auprès :

- de tout prestataire informatique, y compris auprès d'une entité du groupe auquel l'établissement appartient, ~~à condition que~~. Au cas où ces systèmes ~~ne~~ contiennent ~~aucune donnée confidentielle lisible des données confidentielles lisibles~~ concernant les clients. ~~Dans le cas contraire~~, l'établissement ~~s'assure, veille~~ au ~~regard des éventuels risques juridiques et obligations légales, respect des dispositions de l'article 41, paragraphe 2bis~~ de ~~la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles LSF.~~

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

~~191-194.~~ Les services de conseil, de développement et de maintenance peuvent être contractés avec tout prestataire informatique, y compris un service informatique du groupe auquel l'établissement appartient ou un PSF de support.

~~192-195.~~ Des tiers sous-traitants ~~autres que les PSF de support~~ 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. ~~Un accord exprès de l'établissement est nécessaire pour chacune des interventions sur le système de production, à l'exception des interventions réalisées par un PSF de support dans le cadre de son mandat, et que les dispositions de l'article 41, paragraphe 2bis de la LSF soient respectées.~~

~~193-196.~~ Toute modification des fonctionnalités des applications par un tiers - autres que des modifications liées à de la maintenance corrective - doit être soumise pour accord à l'établissement, préalablement à sa mise en production.

~~194-197.~~ L'établissement s'assurera qu'en cas de nécessité, il n'y ait aucun obstacle juridique pour avoir accès aux programmes d'exploitation qui ont été développés par un tiers sous-traitant. Ce but peut être atteint notamment lorsque l'établissement est juridiquement propriétaire des programmes. L'établissement s'assurera de la possibilité de poursuivre l'exploitation des applications critiques à l'activité en cas de défaillance du sous-traitant, pour une période compatible avec un transfert de cette sous-traitance vers un autre sous-traitant ou une reprise en mains propres des applications concernées.

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

~~195-198.~~ 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, seul le personnel du PSF de support ou de l'établissement de crédit luxembourgeois peut indifféremment travailler dans ses locaux ou ceux du professionnel financier sans encadrement particulier de la part du personnel de l'établissement, à condition que la prestation relève de l'article 41(5) de la LSF et fasse l'objet d'un contrat de service permettant cette autonomie. Lorsque le sous-traitant n'est pas PSF de support ou établissement de crédit luxembourgeois, l'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. 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.

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

~~196-199.~~ Il n'est pas exigé que le centre de traitement soit physiquement localisé auprès de l'entité contractuellement responsable de la gestion des systèmes informatiques. Que le centre de traitement soit au Luxembourg ou à l'étranger, il est donc possible que l'hébergement du site soit confié à un autre prestataire que celui qui preste les services de gestion des systèmes informatiques. Dans ce cas, l'établissement doit s'assurer que les principes énoncés dans le présent sous-chapitre sont respectés par l'entité contractuellement responsable de la gestion des systèmes informatiques et que le processus de sous-traitance en cascade est maîtrisé.

~~197-200.~~ Lorsque le centre de traitement est au Luxembourg, il peut être logé auprès d'un prestataire autre qu'un établissement de crédit ou un PSF de support, à condition que celui-ci ~~n'ait aucun n'agisse pas en tant qu'opérateur~~. Si le prestataire a un accès physique ~~et ou~~ logique sur les systèmes de l'établissement, l'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.

~~198-201.~~ Lorsque le centre de traitement est à l'étranger, aucune donnée confidentielle de nature à identifier un client de l'établissement ne peut y être stockée 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 s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier.~~ L'établissement veille au respect des dispositions de l'article 41, paragraphe 2bis de la LSF.

#### **Section 7.4.3. Exigences générales supplémentaires**

~~199-202.~~ Afin de permettre à l'établissement d'apprécier la fiabilité et l'exhaustivité des données produites par le système informatique ainsi que leur compatibilité avec les prescriptions comptables et de contrôle interne, il doit avoir parmi ~~ses employés~~ 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.

~~200-203.~~ En cas de prestation de services informatiques par voie de télécommunication, l'établissement doit s'assurer :

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

~~201-204.~~ L'établissement doit s'assurer que les mécanismes de saisie, d'impression, de sauvegarde, de stockage et d'archivage garantissent la confidentialité des données.

~~202-205.~~ La sous-traitance ne doit pas aboutir à transférer la fonction financière et comptable à un tiers. L'établissement disposera à la fin de chaque jour d'une balance de tous les comptes et de tous les mouvements comptables de la journée. Le système doit permettre de tenir une comptabilité régulière suivant les normes en vigueur au Luxembourg et donc de respecter les règles de forme et de fond imposées par la réglementation comptable luxembourgeoise.

~~203.~~ Lorsque l'établissement opère à l'étranger en recourant aux services d'intermédiaires professionnels (même s'ils font partie du groupe auquel l'établissement appartient) ou lorsqu'il y dispose de succursales ou de bureaux de représentation, tout accès par ces intermédiaires ou les représentants et employés de ces bureaux et succursales à son système d'informations au Luxembourg doit faire l'objet d'une autorisation par la CSSF.

#### **Section 7.4.4. Documentation**

~~204-206.~~ 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 l'organe de surveillance, 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).

~~205-207.~~ 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.

~~206-208.~~ 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

~~207-209.~~ Pour les établissements de crédit, ~~le rapport les rapports~~ ICAAP/ILAAP et l'attestation annuelle de conformité avec les exigences de la présente circulaire, émis par la direction autorisée ~~suivant le point 61~~ ainsi que les rapports de synthèse des fonctions de contrôle interne ~~suivant le point 116~~ sont ~~communiquées communiqués~~ à ~~la~~ l'autorité compétente conformément aux exigences de la circulaire CSSF ensemble avec le projet des comptes annuels à publier (« procédure VISA »). Pour les entreprises d'investissement, ~~ces informations sont soumis à la CSSF dans le mois qui suit la tenue de l'assemblée générale ordinaire ayant approuvé les comptes annuels.~~ 15/602. Les informations en question sont à établir en français, allemand ou anglais.

## Partie III. Gestion des risques

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

Sous-chapitre 1.1. ~~La~~ 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 ~~4.2.3~~ 1.1.2. Politiques spécifiques (de risque, de fonds propres et de liquidités)

3. La politique de risque, qui met en œuvre la stratégie du conseil d'administration définie par l'organe de surveillance 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 la tolérance de l'établissement à l'égard du risque 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, du 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 de l'organe de surveillance 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**

- ~~1-5.~~ 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.
- ~~2-6.~~ 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. ~~Il détermine en particulier ses niveaux de tolérance à l'égard de tous les risques qu'il encourt.~~
- ~~3.~~ ~~La politique de risque explique comment les différents risques sont détectés, mesurés, déclarés, gérés, limités et contrôlés. Elle fixe le processus d'approbation spécifique qui règle la prise de risques (et la mise en œuvre de mesures d'atténuation éventuelles) ainsi que les processus de mesure et de déclaration qui garantissent que l'établissement dispose en permanence d'une vue exhaustive sur l'ensemble de ses risques.~~
- ~~4.~~ ~~Les établissements se dotent d'un système de limites internes et de seuils d'alerte relatifs à l'ensemble de leurs risques.~~
- ~~5-7.~~ ~~La gestion des~~ risques envers des parties liées sont à traiter sur le plan interne comme des risques envers des parties tierces. Le est intégrée dans tous les éléments du dispositif de gouvernance interne ~~leur est applicable dans tous ses éléments.~~

~~Sous-chapitre 1.2. — La mesure des risques~~

~~6-8.~~ 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.

~~7-9.~~ 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.

~~8-10.~~ 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 l'organe de surveillance~~ 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

~~9-11.~~ Les risques de concentration résultent notamment ~~de positions d'expositions~~ importantes ~~(«concentrées»)~~ sur des clients ~~ou, des~~ contreparties ou des fournisseurs de services respectivement des groupes de clients ~~ou, contreparties ou fournisseurs de services~~ liés, y compris des parties liées, sur des pays ou des secteurs (industries) ~~ainsi que ou encore~~ sur des produits ou des marchés spécifiques (concentration intra-risque). ~~Ces positions peuvent être des postes d'actif, de passif ou de hors-bilan, mais les risques de concentration~~ Ces expositions ne se ~~réfèrent 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.

12. Pour les établissements actifs sur le marché domestique, il existe généralement une exposition concentrée sur le marché immobilier luxembourgeois. Un retournement significatif de ce marché serait de nature à porter atteinte à la stabilité financière de ces établissements et à impacter négativement l'image de la place financière luxembourgeoise dans son ensemble. Il importe dès lors que les établissements mettent en œuvre des politiques prudentes en matière d'octroi de crédits immobiliers, conformément aux sous-chapitres 3.2 et 3.3.

~~10. Les points 211 à 215 s'appliquent en particulier aux risques de concentration.~~

### Chapitre 3. Risque de crédit

#### Sous-chapitre 3.1. Principes généraux<sup>15</sup>

13. Par prise de risque au sens du présent sous-chapitre, il faut comprendre non seulement les décisions en matière de nouveaux crédits à accorder, mais également les décisions prises dans la cadre de la restructuration ou de la renégociation de crédits existants, notamment à la suite d'une détérioration significative de la solvabilité du débiteur. Les restructurations et renégociations comprennent notamment l'octroi de prorogations, de reports, de renouvellements ou de réaménagements de conditions de crédit, y compris le plan de remboursement et toutes mesures de renégociation au sens de l'article 49b du CRR et les prêts non performants au sens de l'article 47a.(3) du CRR.

~~14.~~ 14. Chaque prise de risque de crédit doit faire l'objet d'une analyse écrite qui porte au moins sur la solvabilité du débiteur, sur le plan de remboursement et sur la capacité de remboursement de l'emprunteur sur toute la durée de l'emprunt. En particulier, la décision de crédit ne peut pas reposer que sur une analyse exclusive des sûretés ou autres techniques d'atténuation de risque de crédit. Les établissements prennent en compte le niveau d'endettement global de l'emprunteur du débiteur, respectivement du groupe de débiteurs liés.

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

<sup>15</sup> Complétant les dispositions de l'article 9 du RCSSF 15-02 en matière de risque de crédit et de contrepartie.

~~12-15.~~ Chaque prise de risque de crédit doit faire l'objet d'un processus décisionnel prédéfini qui englobe également une instance différente de la fonction commerciale.

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

Il appartient aux établissements de définir en interne la notion de risque de crédit de « faible importance » pour les besoins du ~~premier~~ paragraphe précédent. Cette définition s'oriente en particulier au moins à la capacité de l'établissement à gérer, à supporter et à contrôler ces risques. ~~Les établissements disposent d'une part, et du montant de politiques claires qui définissent les mesures à prendre lorsqu'un/une exposition et de la qualité de crédit du débiteur ne respecte pas ou signale à la banque qu'il n'est plus en mesure de respecter les clauses contractuelles de son engagement, notamment les différentes échéances et de paiement, la transaction d'autre part.~~

~~13.~~ Chaque décision de restructuration d'un crédit fait l'objet du processus décisionnel énoncé aux points 221 à 223. Les établissements maintiennent une liste reprenant l'ensemble des crédits restructurés.

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

~~14.~~ Les établissements disposent d'un solide dispositif pour la détection et la gestion des engagements en retard de paiement. Les engagements en retard de paiement sont les engagements dont les échéances contractuelles définies pour le paiement du capital et/ou des intérêts sont dépassées.

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

~~15.~~ Les établissements doivent maintenir une liste des engagements douteux sur un débiteur ou groupe de débiteurs liés. ~~Ces engagements font l'objet d'une revue périodique et objective qui doit permettre à l'établissement de reconnaître et d'effectuer les provisions et dépréciations d'actifs qui s'imposent.~~

**Précision:**

~~Pour les établissements actifs sur le marché domestique, il existe généralement une exposition concentrée sur le marché immobilier luxembourgeois. Un retournement significatif de ce marché, très difficile à prédire par ailleurs, serait de nature à porter atteinte à la stabilité financière de ces établissements et à impacter négativement l'image de la place financière luxembourgeoise dans son ensemble. Il importe dès lors que les établissements mettent en œuvre des politiques prudentes en matière d'octroi de crédits immobiliers, conformément au sous-chapitre 3.1 et au point 228. Par ailleurs, les établissements doivent disposer de fonds propres suffisants pour faire face à des développements adverses du marché immobilier résidentiel. Les exigences codifiées au point 229 entendent ainsi renforcer la stabilité financière de ces établissements par le biais d'exigences de fonds propres réglementaires dûment ajustées pour le risque. Ces exigences constituent un renforcement des règles actuelles contenues dans la circulaire CSSF 06/273 suivant les leçons tirées des épisodes récentes de crises financières. Ainsi, suivant le premier tiret du point 229, les établissements utilisant l'approche standard pour le risque de crédit ne peuvent appliquer dorénavant le taux de pondération préférentiel de 35% qu'aux seules parts de leurs crédits hypothécaires dont le rapport « loan to value » (LTV) est inférieur à 80% (crédits dont « la valeur du bien immobilier dépasse de 25% au moins celle de l'exposition »). Ainsi un crédit hypothécaire, qui remplit toutes les conditions d'éligibilité de la section 2.2.7.1 de la partie VII de la circulaire CSSF 06/273 (exposition sur la clientèle de détail pondérée à 75%) et les critères de la section 2.2.8.1 de la partie VII de cette même circulaire (pondération préférentielle à 35%) à l'exception du nouveau critère 41, lit. d) qui limite le LTV à 80%, est dorénavant pondéré pour les besoins de la détermination des exigences de fonds propres réglementaires à  $(0,8/LTV) * 35\% + ((LTV - 0,8)/LTV) * 75\%$  au lieu de 35%. La part du crédit dépassant 80% de la valeur de l'objet immobilier est à pondérer suivant la classe d'exposition sous-jacente. Dans le cas sous rubrique, l'exposition satisfait tous les critères d'appartenance aux expositions sur la clientèle de détail et la pondération à risque s'établit par conséquent à 75%. Pour la détermination du LTV, les établissements peuvent prendre en considération tous les facteurs d'atténuation du risque – apport personnel direct de la part de l'emprunteur ou encore intervention de tiers par le biais d'apports, de sûretés réelles ou encore de garanties réelles ou personnelles dans les conditions prévues à la partie IX de la circulaire CSSF 06/273 (« reconnaissance des techniques d'atténuation du risque de crédit »). Pour les établissements utilisant l'approche fondée sur les notations internes et suivant le deuxième tiret du point 229, le seuil du « plancher » pour le taux de perte en cas de défaut est maintenu à 10% après le 31 décembre 2012.~~

Ces établissements doivent également soumettre leur adéquation réglementaire de fonds propres à un test d'endurance qui respecte au moins les paramètres inscrits au troisième tiret du point 229.

16. Les établissements appliquent une politique d'octroi de crédits prudente qui est de nature à préserver leur stabilité financière indépendamment de l'évolution observée ou attendue du marché immobilier résidentiel. Cette politique s'articule notamment autour ~~d'un rapport sain de valeurs saines des taux d'endettement et des ratios~~ entre la charge de la dette et le revenu sur la durée du crédit ainsi qu'entre le montant du crédit accordé et la valeur des garanties obtenues (« loan-to-value »), y compris l'hypothèque sur l'immeuble sous-jacent, basée sur des méthodes d'évaluations prudentes.

~~17. La partie VII de la circulaire CSSF 06/273 est modifiée comme suit :~~

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

### Sous-chapitre 3.3. Crédits aux promoteurs immobiliers

~~18-17.~~ Chaque financement d'un projet de promotion immobilière doit prévoir au moment de l'octroi du crédit une date de commencement du remboursement du principal. Cette date ne peut pas dépasser un délai raisonnable par rapport au début du financement du projet. Un dépassement de ce délai implique automatiquement le classement du dossier dans la liste des crédits restructurés (voir le point 225) « en défaut » au sens de l'article 178 du CRR, de l'article 14 du règlement CSSF 18-03 et des EBA/GL/2016/07 et le provisionnement intégral des intérêts impayés.

Le financement de la promotion immobilière ne doit pas se faire sur simple notoriété du promoteur. ~~Il doit~~ il doit en particulier considérer l'ensemble des autres facteurs permettant d'évaluer la solidité du promoteur, la structuration juridique ainsi que la solidité financière des projets, l'environnement dans lequel les projets se réalisent, leurs phases de développement et l'ensemble des garanties et assurances qui s'y rapportent.

Le financement doit par ailleurs être couvert, en sus de l'hypothèque sur l'objet financé, par une garantie personnelle du promoteur à moins que d'autres garanties ou sûretés ne couvrent significativement le coût total de l'objet financé.

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

Il est rappelé que les financements spéculatifs de biens immobiliers tels que définis à l'article 4, paragraphe 1, point 79) du CRR sont considérés comme des expositions présentant un risque particulièrement élevé. A ce titre, ils reçoivent une pondération de risque de 150% tel que défini à l'article 128, paragraphe 2, point d) du CRR sous l'approche standard pour le risque de crédit.

#### Sous-chapitre 3.4. Expositions présentant un risque particulièrement élevé

18. Les établissements qui appliquent l'approche standard pour le risque de crédit mettent en place un processus pour l'identification des expositions présentant un risque particulièrement élevé. Ce processus couvre au moins les expositions au sens de l'article 128, paragraphes 2 et 3 du CRR.

19. Les établissements appliquent les orientations EBA/GL/2019/01 qui précisent les notions d'investissement dans des entreprises de capital risque et d'investissement en capital-investissement, telles que visées à l'article 128, paragraphe 2, points a) et c) du CRR. Ces orientations précisent également quels types d'expositions, autres que ceux mentionnés à l'article 128, paragraphe 2 du CRR, doivent être considérés comme présentant un risque particulièrement élevé et dans quelles circonstances.

Les types d'expositions identifiés par les établissements qui présentent un risque de perte particulièrement élevé, sans pour autant répondre aux caractéristiques spécifiques décrites dans les EBA/GL/2019/01, doivent être notifiés à l'autorité compétente, en utilisant le formulaire correspondant disponible sur le site internet de la CSSF.

#### Sous-chapitre 3.5. Expositions non performantes et expositions restructurées

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

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

En complément, les établissements disposent d'un solide dispositif pour la détection, la gestion et le provisionnement de l'ensemble des engagements « en défaut » au sens de l'article 178 du CRR, de l'article 14 du règlement CSSF 18-03 et des EBA/GL/2016/07.

21. Les établissements doivent maintenir une liste des engagements sur un débiteur ou un groupe de débiteurs liés, qu'ils soient restructurés au sens de l'article 49b. du CRR, non-performants au sens de l'article 47a.(3) du CRR et « en défaut ». Ces engagements font l'objet d'une revue périodique et objective qui doit permettre à l'établissement de reconnaître et d'effectuer les provisions et dépréciations d'actifs qui s'imposent.

22. Les établissements doivent disposer de pratiques appropriées de gouvernance et de gestion des risques de leurs expositions non performantes<sup>16</sup>, de leurs expositions restructurées<sup>17</sup> et des actifs saisis, afin de réduire efficacement et durablement les expositions non performantes de leurs bilans conformément aux exigences de la circulaire 20/751.

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

~~19-23.~~ 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 ~~la tolérance à l'égard du~~ l'appétit au risque et au principe d'une gestion saine et prudente des affaires.

~~20-24.~~ Le mécanisme de tarification est approuvé par la direction autorisée et surveillé par la fonction de contrôle des risques. Les prix de transfert doivent être transparents et communiqués aux ~~employés-membres~~ concernés du personnel. La comparabilité et la cohérence des systèmes des prix de cession interne utilisées au sein du groupe doit être assurée.

~~21-25.~~ 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.

<sup>16</sup> Expositions classées comme non performantes conformément à l'annexe V du règlement d'exécution (UE) n° 680/2014 de la Commission.

<sup>17</sup> Expositions pour lesquelles des mesures de renégociation ont été appliquées conformément à l'annexe V du règlement d'exécution (UE) n° 680/2014 de la Commission.

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

26. L'activité de banque privée est particulièrement exposée aux risques de blanchiment de capitaux et le financement du terrorisme. En conséquence, les établissements 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.

~~22-27.~~ Les établissements disposent de processus solides pour garantir que les relations d'affaires avec leurs clients ~~sont-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.

~~23-28.~~ Les établissements disposent de processus solides pour garantir le respect des profils de risque des clients, dans le but notamment de respecter les exigences découlant de la réglementation « MiFID ».

~~24-29.~~ Les établissements disposent de processus solides pour garantir la communication d'informations correctes aux clients sur l'état de leurs avoirs. La production et la distribution des relevés de comptes et de toute autre information sur l'état des avoirs doivent être séparées de la fonction commerciale.

~~25-30.~~ Les ~~versements-entrées~~ et ~~retraits-d'objets-sorties physiques d'espèces, de titres ou d'autres objets~~ de valeur ~~(par exemple les espèces et titres au porteur)~~ doivent être effectués ou contrôlés par une fonction séparée de la fonction commerciale.

~~26-31.~~ L'encodage et la modification des données signalétiques des clients doit être effectuée ou contrôlée par une fonction indépendante de la fonction commerciale.

~~27-32.~~ 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.

~~29-33.~~ Les établissements doivent disposer d'un processus solide d'encadrement des crédits et dépassements en compte courant dans le cadre de l'activité de banque privée. Les garanties financières couvrant ces crédits doivent être suffisamment diversifiées et liquides. Dans le but de disposer d'une marge de sécurité adéquate, des décotes prudentes doivent être appliquées en fonction de la nature des garanties financières. Les établissements doivent disposer d'un « early warning system » indépendant de la fonction commerciale qui organise la surveillance de la valeur des garanties financières et déclenche le processus de liquidation des garanties financières. Il doit être assuré que le processus de liquidation soit déclenché suffisamment à temps et en tout cas avant que la valeur des garanties ne devienne inférieure au crédit. Les contrats avec les clients doivent décrire clairement la procédure déclenchée en cas d'insuffisance des garanties.

## Chapitre 6. Risques liés aux entités shadow banking

~~29.~~ Ce chapitre s'applique uniquement aux établissements auxquels s'applique la quatrième partie (grands risques) du règlement (UE) n° 575/2013, conformément au niveau d'application prévu à la première partie, titre II, dudit règlement.

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

~~30-34.~~ Les établissements mettent en place un cadre interne dédié permettant de recenser, de gérer, de contrôler et d'atténuer les risques liés aux expositions sur les entités dites « entités du système bancaire parallèle » (« entités shadow banking »<sup>18</sup>) conformément aux EBA/GL/2015/20.

<sup>18</sup> 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 ».

31-35. Les établissements appliquent un seuil de matérialité dédié pour identifier les expositions sur des entités shadow banking. Conformément aux EBA/GL/2015/20, toute exposition individuelle sur une entité shadow banking qui est supérieure ou égale à 0,25%<sup>19</sup> des fonds propres éligibles de l'établissement<sup>20</sup>, après prise en compte des effets d'atténuation du risque de crédit et des exemptions<sup>21</sup>, doit être prise en considération et ne peut pas être considérée comme une exposition de « faible importance ».

32-36. Les établissements veillent à ce que les risques éventuels pour l'établissement en raison de leurs différentes expositions sur des entités shadow banking soient pris en compte de manière adéquate dans le processus d'évaluation de l'adéquation du capital interne (ICAAP) de l'établissement et dans la planification du capital.

#### Sous-chapitre 6.2. Application de limites quantitatives

33-37. Les établissements limitent leurs expositions sur des entités shadow banking conformément à l'une des deux approches (approche de base ou approche de repli) telles que définies dans les **orientations**-EBA/GL/2015/20.

34-38. Conformément à l'approche de base, les établissements doivent fixer une limite agrégée pour leurs expositions sur des entités shadow banking par rapport à leurs fonds propres éligibles.

35-39. Dans sa fixation d'une limite agrégée pour les expositions sur des entités shadow banking, chaque établissement doit tenir compte de :

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

36-40. Indépendamment de la limite agrégée et en plus de celle-ci, les établissements doivent fixer des limites plus strictes pour leurs expositions individuelles sur des entités shadow banking.

<sup>19</sup> Au sens de la définition des « Expositions sur des entités du système bancaire parallèle » du paragraphe 11 des EBA/GL/2015/20.

<sup>20</sup> Au sens de l'article 4, paragraphe 1, point 71 du CRR.

<sup>21</sup> i) Effets d'atténuation du risque de crédit conformément aux articles 399 et 403 du CRR,

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

37-41. Lorsqu'ils fixent ces limites, dans le cadre de leur processus d'évaluation interne, les établissements doivent tenir compte :

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

38-42. Dans le cas où, les établissements ne sont pas en mesure d'appliquer l'approche de base telle que décrite ci-avant, les expositions agrégées sur des entités shadow banking doivent être soumises aux limites aux grands risques conformément à l'article 395 ~~règlement (UE) n° 575/2013 du CRR~~ (ci-après « approche de repli »).

39-43. L'approche de repli doit être appliquée comme suit :

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

- Si certains établissements peuvent satisfaire aux exigences concernant les processus et les mécanismes de contrôle efficaces ou la supervision par leur organe de direction, telles que prévues au sous-chapitre 6.1, mais ne peuvent réunir suffisamment d'informations pour leur permettre de fixer des limites appropriées, comme prévu ~~à la section au sous-chapitre 6.2-4~~, ils ne doivent appliquer l'approche de repli qu'aux expositions sur des entités shadow banking pour lesquelles les établissements ne peuvent réunir suffisamment d'informations. L'approche de base telle que décrite ~~à la section au sous-chapitre 6.2-4~~ doit être appliquée aux expositions restantes sur des entités shadow banking.

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

~~40.—Ce chapitre s'applique uniquement aux établissements de crédit.~~

~~41-44.~~ Les établissements mettent en place des politiques de gestion des risques afin de définir leur approche de la charge pesant sur les actifs, de même que des procédures et contrôles qui garantissent que les risques associés à la gestion des garanties et à la charge pesant sur les actifs sont adéquatement identifiés, suivis et gérés. Il convient que ces politiques tiennent compte de leur modèle ~~d'activité d'activités~~, des États membres dans lesquels ils opèrent, des spécificités des marchés du financement et de la situation macroéconomique. Ces politiques doivent être approuvées ~~conformément aux dispositions du point 19 par l'organe de surveillance~~.

~~42-45.~~ Les établissements instituent un cadre de suivi général qui fournit des informations en temps utile, au moins une fois par an, à la direction autorisée et ~~au conseil d'administration à l'organe de surveillance~~ sur :

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

~~43-46.~~ Les établissements incluent dans leurs plans de continuité des actions pour faire face à la charge pesant sur les actifs éventuelle résultant d'événements sources de tensions, à savoir de chocs plausibles bien que peu probables, y compris les dégradations des notations des établissements de crédit, les dévaluations des actifs nantis et les augmentations des exigences de marge.

**Précision :**

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

## Chapitre 8. Risque de taux d'intérêt

Sous-chapitre 8.1 Risque de taux d'intérêt inhérent aux activités autres que de négociation

~~44-47.~~ Dans leur mise en œuvre de l'article 14 (Risque de taux d'intérêt inhérent aux activités hors portefeuille de négociation) du règlement CSSF N° 15-02 relatif au processus de contrôle et d'évaluation prudentiels s'appliquant aux établissements CRR, les établissements CRR se conforment aux orientations que l'Autorité bancaire européenne a publiées en la matière<sup>22</sup>. Ne sont donc pas visées par le présent chapitre, les entreprises d'investissement qui ne sont pas des entreprises d'investissement CRR RCSSF 15-02, les établissements se conforment aux EBA/GL/2018/02.

Sous-chapitre 8.2. Corrections de la durée modifiée des titres de créance

~~45-48.~~ Ces orientations comprennent Les établissements qui appliquent l'approche standard pour le calcul de leurs des exigences de haut niveau et des exigences détaillées qui visent les trois domaines suivants : les fonds propres internes alloués au risque de taux d'intérêt du portefeuille liées au risque de taux d'intérêt général sont tenus d'appliquer des modifications au calcul de la durée pour tenir compte du risque de remboursement anticipé des titres de créance. Les établissements appliquent l'une des deux méthodes de correction de la durée modifiée prévues par les EBA/GL/2016/09.

<sup>22</sup> « Orientations sur la gestion du risque de taux d'intérêt inhérent aux activités autres que de négociation » (EBA/GL/2015/09) accessibles sur le site internet de l'EBA à l'adresse suivante : <https://www.eba.europa.eu/eba-updates-guidelines-on-interest-rate-risk-arising-from-non-trading-activities>

## Chapitre 9. Risques liés à la conservation d'actifs financiers par des tiers

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

## Partie IV. Chronologie

- Circulaire CSSF 12/552, transposant les lignes directrices de l'Autorité bancaire (« IRRBB 1 »), la mesure de ce risque (« IRRBB 2 » et « IRRBB 3 ») ainsi que le dispositif européenne (EBA) en matière de gouvernance interne relatif au risque de taux d'intérêt du portefeuille 27 septembre 2011 (EBA Guidelines on Internal Governance, « GL 44 »), celles du Comité de Bâle sur le contrôle bancaire (« IRRBB 4.1 » et « IRRBB 4.2 »). (BCBS) en matière d'audit interne du 28 juin 2012, les lignes directrices du CEBS publiées le 26 avril 2010 (Principles for disclosures in times of stress (Lessons learnt from the financial crisis)), les lignes directrices du CEBS du 2 septembre 2010 en matière de risques de concentration (CEBS Guidelines on the management of concentration risk under the supervisory review process, « GL31 ») et les lignes directrices du 27 octobre 2010 en matière de tarification de la liquidité (Guidelines on Liquidity Cost Benefit Allocation).

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

- ~~46. La présente circulaire est applicable à partir du 1<sup>er</sup> juillet 2013.~~
- ~~Par dérogation au premier paragraphe, les dispositions suivantes sont d'application à partir du 1<sup>er</sup> janvier 2014 :~~
- ~~Section 4.1.2 (Composition et qualification du conseil d'administration) ;~~
  - ~~Section 4.1.4 en ce qui concerne les comités spécialisés, à l'exception du comité d'audit ;~~

- ~~• Point 32 (Interdiction de cumuler les mandats de président du conseil d'administration et de directeur agréé) ;~~
- ~~• La nécessité de fixer par écrit les lignes directrices prévues aux tirets 4 à 8 du point 17.~~
- ~~47. CSSF 12/552 annule et remplace~~ les circulaires IML 93/94 et CSSF 10/466 ~~sont abrogées à partir du 1<sup>er</sup> juillet 2013.~~
- ~~48-52. , ainsi que~~ les circulaires IML 95/120, IML 96/126, IML 98/143, CSSF 04/155 et CSSF 05/178 ~~ne sont plus applicables aux dans le chef des~~ établissements de crédit ~~et entreprises d'investissement à partir du 1<sup>er</sup> juillet 2013.~~
- ~~49. Mises à jour successives :~~
  - Circulaire CSSF 13/563 transposant les orientations de l'EBA en matière d'éligibilité des administrateurs, directeurs autorisés et responsables de fonctions ~~clés~~ du 22 novembre 2012 (*Guidelines on the assessment of the suitability of members of the management body and key function holders* — « EBA/GL/2012/06 ») ainsi que les orientations du 6 juillet 2012 de l'ESMA concernant certains aspects de la directive MIF relatifs aux exigences à l'encontre de la fonction compliance (Guidelines on certain aspects of the MiFID compliance function requirements — « ESMA/2012/388 »).  
~~Les orientations précitées sont disponibles sur le site de l'EBA (www.eba.europa.eu) et de l'ESMA (www.esma.europa.eu).~~
  - Circulaire CSSF 14/597 transposant la recommandation du Comité Européen du Risque Systémique (CERS) sur le financement des établissements de crédit (« CERS/2012/2 »), sous-recommandation B concernant la mise en place d'un cadre général de gestion du risque de charge pesant sur les actifs (« asset encumbrance »).  
~~La recommandation précitée est disponible sur le site du CERS (www.esrb.europa.eu).~~
  - Circulaire CSSF 16/642 transposant les orientations de l'EBA en matière de gestion du risque de taux d'intérêt inhérent aux activités autres que de négociation (Guidelines on the management of interest rate risk arising from non-trading activities — « EBA /GL/2015/08 »).
  - Circulaire CSSF 16/647 transposant les orientations de l'EBA en matière de limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013 (Guidelines on limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation (EU) No 575/2013 — « EBA/GL/2015/20 »).

- Circulaire CSSF 20/750 transposant les orientations de l'EBA relatives à la gestion des risques liés aux technologies de l'information et de la communication et à la sécurité (Guidelines on ICT and security risk management, EBA/GL/2019/04)
- Circulaire CSSF XX/XXX transposant les orientations de l'EBA en matière de gouvernance interne découlant de la directive 2013/36/UE (Guidelines on internal governance under Directive 2013/36/EU, « EBA/GL/2017/11 »), les orientations conjointes de l'EBA et de l'ESMA sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés (Guidelines on the assessment of the suitability of members of the management body and key function holders, « EBA/GL/2017/12 »), les orientations de l'EBA sur l'application de la définition du défaut au titre de l'article 178 du règlement (UE) n° 575/2013 (Guidelines on the application of the definition of default under Article 178 of Regulation (EU) No 575/2013 « EBA/GL/2016/07 »), les orientations de l'EBA sur la spécification des types d'expositions devant être considérés comme présentant un risque élevé (Guidelines on specification of types of exposures to be associated with high risk « EBA/GL/2019/01 »), les 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 »), et les orientations de l'EBA sur les corrections de la durée modifiée des titres de créance en vertu de l'article 340, paragraphe 3, deuxième alinéa, du règlement (UE) n° 575/2013 (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 »).

Les lignes directrices, orientations, et recommandations précitées peuvent être consultées et téléchargées sur les sites internet respectifs de l'EBA ([www.eba.europa.eu](http://www.eba.europa.eu)), de l'ESMA ([www.esma.europa.eu](http://www.esma.europa.eu)), du BCBS (<https://www.bis.org/bcbs/index.htm>) et du CERS ([www.esrb.europa.eu](http://www.esrb.europa.eu)). Les orientations précitées sont disponibles sur le site de l'EBA ([www.eba.europa.eu](http://www.eba.europa.eu)).

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](mailto:direction@cssf.lu)  
[www.cssf.lu](http://www.cssf.lu)