Commission de Surveillance
du Secteur Financier

Circulaire CSSF 26/906

Administration centrale, gouvernance interne et gestion des risques

Circulaire CSSF 26/906

Administration centrale, gouvernance interne et gestion des risques

À tous les établissements de paiement et établissements de monnaie électronique

Luxembourg, le 20 janvier 2026

Mesdames, Messieurs,

Les articles 11, paragraphe 2 et 24-7, paragraphe 2, de la loi modifiée du 10 novembre 2009 relative aux services de paiement (« LSP ») exigent des établissements de paiement et des établissements de monnaie électronique, compte tenu de la nécessité de garantir la gestion saine et prudente de ces établissements, 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, ainsi que des mécanismes de contrôle et de sécurité de leurs systèmes informatiques.

L'octroi et le maintien de l'enregistrement des prestataires de services d'information sur les comptes requiert en référence aux articles 48-1*bis* et 8, paragraphe 1, lettre e), de la LSP que ces prestataires de services d'information sur les comptes disposent d'un dispositif de gouvernance interne et de mécanismes de contrôle incluant notamment des procédures administratives, de gestion des risques et comptables, qui démontrent que ce dispositif de gouvernance interne, ces mécanismes de contrôle et ces procédures sont proportionnés, adaptés, sains et adéquats. De ce fait, la présente circulaire s'applique aux prestataires de services d'information sur les comptes, aux fins de laquelle ils sont traités comme des établissements de paiement tout en tenant compte de l'application du principe de proportionnalité.

Dans le passé, la Commission de Surveillance du Secteur Financier (« CSSF ») avait précisé les modalités d'application de ces articles dans différentes circulaires. La CSSF a décidé de consolider l'ensemble des modalités d'application clés en matière de d'administration centrale, de gouvernance interne et de gestion des risques dans une circulaire unique.

Cette circulaire prend en compte les orientations de l'Autorité Bancaire Européenne sur les informations à fournir pour l'agrément d'établissements de paiement et d'établissements de monnaie électronique et pour l'enregistrement de prestataires de services d'information sur les comptes au titre de l'article 5, paragraphe 5, de la directive (UE) 2015/2366 (EBA/GL/2017/09)[1].

Les circulaires IML 95/120, IML 96/126, IML 98/143 et CSSF 04/155 seront abrogées dans le chef des établissements de paiement et des établissements de monnaie électronique et les circulaires CSSF 11/510 et CSSF 11/520 seront modifiées.

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 ceux de la gestion des risques liés aux technologies de l'information et de la

[1] Ces orientations sont adoptées au Luxembourg au travers de la circulaire CSSF 18/677.

communication (TIC), de la notification d'incidents majeurs, de la rémunération ou de l'externalisation qui sont couverts par des circulaires distinctes.

Lorsqu'en réponse à des développements réglementaires sur le plan européen, international ou national, la CSSF est amenée à préciser les exigences reprises dans la présente circulaire, elle procédera à la mise à jour de cette circulaire.

TABLE DES MATIÈRES

Partie I. Définitions et champ d'application

Chapitre 1. Définitions

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

1) « établissement » : un établissement de paiement ou un établissement de monnaie électronique conformément au paragraphe 2 du chapitre 2 de la partie I « Champ d'application et proportionnalité » ;

2) « établissement de paiement » : les personnes visées à l'article 1er, point 18), de la LSP ;

3) « établissement de monnaie électronique » : les personnes visées à l'article 1er, point 17), de la LSP ;

4) « fonctions de contrôle interne » : la fonction compliance, la fonction d'audit interne et la fonction de contrôle des risques ;

5) « LSP » : la loi modifiée du 10 novembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres ;

6) « organe de surveillance » : l'organe ou à défaut les personnes qui du point de vue du droit des sociétés contrôlent la gestion exercée par l'organe de gestion. Le terme « organe de surveillance » correspond généralement au conseil d'administration. Toutefois, ce terme n'est pas à prendre dans son acception juridique, puisque les établissements 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 » ;

7) « organe de gestion » : les personnes visées aux articles 8, paragraphe 1), lettre i) et 24-4, lettre i), de la LSP. Ces personnes sont généralement désignées par « dirigeants », « directeur(s) autorisé(s) » ou « direction autorisée » ;

8) « parties liées » :

   a. les entités (structures) juridiques appartenant au groupe auquel l'établissement appartient ;

   b. les actionnaires ;

   c. les membres de l'organe de gestion ou de surveillance de l'établissement ou des entités mentionnées au point a., leurs conjoints ou partenaires enregistrés conformément au droit national applicable et leurs enfants et parents ;

   d. les entités commerciales dans lesquelles un membre de l'organe de gestion ou de surveillance, ou un membre proche de sa famille tel que visé au point c., détient une participation qualifiée représentant au moins 10 % du capital ou des droits de vote, dans laquelle ces personnes peuvent exercer une influence notable ou dans laquelle ces personnes occupent des postes au sein de l'organe de gestion ou de surveillance ;

9) « prestataires de services d'information sur les comptes » : les personnes visées à l'article 1, point 37*quinquies*), de la LSP ;

10) « utilisateurs de services de paiement » : les personnes visées à l'article 1er, point 46), de la LSP ainsi que les détenteurs de monnaie électronique ;

11) « succursale » : les sièges d'exploitation visés à l'article 1er, point 39), de la LSP ;

12) « personnel » ou « membres du personnel » : l'ensemble des employés de l'établissement y inclus les employés des succursales, bureaux de représentation ou autre siège rattaché à l'établissement. Les personnes mises à la disposition d'un établissement dans le cadre d'un contrat avec un employeur tiers sont également considérées comme des membres du personnel ;

13) « procédures » : l'ensemble, au sens large, des mesures, instructions et règles qui régissent l'organisation et le fonctionnement interne d'un établissement.

Chapitre 2. Champ d'application et proportionnalité

2. La présente circulaire s'applique aux établissements de paiement et aux établissements de monnaie électronique pour lesquels l'État membre d'origine est le Luxembourg, y compris à leurs succursales, ainsi qu'aux succursales luxembourgeoises d'établissements de paiement et d'établissements de monnaie électronique dont l'État d'origine se situe en dehors de l'Espace économique européen et également aux prestataires des services d'information sur les comptes.

   Pour les domaines où la CSSF conserve une responsabilité de contrôle en tant qu'autorité compétente de l'État membre d'accueil – il s'agit notamment des mesures en matière de lutte contre le blanchiment et le financement du terrorisme, des recours extrajudiciaires – les succursales luxembourgeoises d'établissements de paiement et d'établissements de monnaie électronique originaires d'un État membre de l'Espace économique européen mettent en place un dispositif en matière d'administration centrale et de gouvernance interne ainsi qu'une gestion des risques qui sont comparables à ceux prescrits par la présente circulaire.

3. Les établissements tiennent compte de leur taille et de leur organisation interne ainsi que de la nature, de l'échelle et de la complexité de leurs activités et des risques des services qu'ils fournissent lorsqu'ils élaborent et mettent en œuvre leur dispositif de gouvernance interne.

   En pratique, l'application du principe de proportionnalité conduit certains établissements à se doter d'un dispositif renforcé en matière d'administration centrale, de gouvernance interne et de gestion des risques. Ce dispositif renforcé peut comprendre, par exemple, l'instauration de comités spécialisés, la nomination de membres additionnels à l'organe de surveillance ou encore à l'organe de gestion.

   À l'opposé, pour des établissements dont la taille ainsi que la nature, l'échelle et la complexité des activités sont moindres (par exemple les prestataires de services d'information sur les comptes), le principe de proportionnalité peut jouer à la baisse sans préjudice du respect des dispositions légales et en conformité avec les exigences de la présente circulaire.

   L'application à la baisse du principe de proportionnalité est limitée en particulier par le principe de la ségrégation des tâches qui exige que les tâches et responsabilités doivent être attribuées de façon à éviter les conflits d'intérêts dans le chef d'une même personne. Au niveau de l'organe de gestion, alors que la répartition des tâches s'effectue dans le respect du principe de la ségrégation des tâches, la responsabilité reste collective.

Aux fins de l'application du principe de proportionnalité et afin de garantir une mise en œuvre adéquate des exigences légales et réglementaires y compris aux exigences de la présente circulaire, les établissements tiennent notamment compte des aspects/critères suivants :

- les risques et la complexité liés aux types de produits offerts et de services prestés et en particulier la fourniture de services autres que la prestation de services de paiement ou de monnaie électronique y inclus la prestation de service de change, l'octroi de crédits liés aux services de paiement, le cumul de plusieurs autorisations issues du secteur financier, etc. ;
- le volume des opérations de paiement et de monnaie électronique (> EUR 10 milliards) ;
- la taille de l'établissement selon le chiffre d'affaires et le total de bilan (> EUR 0,5 milliard) ;
- le type et le nombre d'utilisateurs des services de paiement ;
- le nombre d'employés de l'établissement (c.-à-d. > 50 personnes) ;
- le réseau de distribution (reposant sur plus d'une succursale ou un réseau d'agents, distributeurs ou des bureaux de représentation) ;
- la taille du groupe (structure d'actionnariat auquel l'établissement appartient) ;
- le nombre et la complexité des schémas d'externalisation y inclus au niveau des systèmes et technologies informatiques (et en particulier le niveau de dépendance et de concentration des schémas d'externalisation) ; et
- la structure de l'architecture des systèmes informatiques (y inclus la continuité des systèmes).

4. Ainsi, quelle que soit l'organisation retenue, les arrangements en la matière doivent permettre à l'établissement d'opérer dans le plein respect des dispositions prévues à la partie II de la présente circulaire. Les établissements documentent par écrit leur analyse en matière de proportionnalité et en font approuver les conclusions par l'organe de surveillance au moins une fois par an.

Partie II. Dispositif en matière d'administration centrale, de gouvernance interne et de gestion des risques

Chapitre 1. L'administration centrale

5. Les articles 11, paragraphe 1), et 24-7, paragraphe 1), de la LSP requièrent que les établissements disposent au Luxembourg d'une administration centrale et du siège statutaire de l'établissement. Cette exigence signifie qu'un établissement ne peut pas se limiter à avoir au Luxembourg un siège juridique (« registered office », « Zulassungssitz »). Il doit y avoir également au Luxembourg son centre de prise de décision et son centre administratif (« head office », « effektiver Sitz »).

6. La notion d'administration centrale comporte deux éléments :

- l'« administration » qui englobe au sens large les organes d'administration et de gestion, les fonctions d'exécution et de contrôle interne ;
- le « centre » qui signifie l'endroit vers lequel tendent et à partir duquel rayonnent les différents éléments de l'ensemble d'une entreprise.

7. Le centre de prise de décision comprend l'organe de surveillance et les personnes (au minimum deux) membres de l'organe de gestion, chargées de la gestion de l'établissement et qui doivent être habilitées à déterminer effectivement l'orientation de son activité. Il inclut également les responsables des fonctions de contrôle interne, des fonctions commerciales ainsi que des différentes fonctions administratives, informatiques et opérationnelles existant à l'intérieur de l'établissement.

   Le centre administratif comprend l'organisation administrative, comptable et informatique qui assure en permanence la bonne administration des valeurs et des biens, l'exécution adéquate des opérations, l'enregistrement correct et exhaustif des opérations et la production d'une information de gestion correcte, complète, pertinente, compréhensible et disponible sans délai. L'administration centrale permet à l'établissement d'atteindre toutes formes d'implantation de l'établissement et en particulier les succursales de l'établissement afin de leur fournir toute information nécessaire ou pertinente à la gestion saine et prudente de l'établissement. La notion d'information de gestion s'entend au sens le plus large, incluant l'information financière et le reporting légal, le cas échéant.

   Sans préjudice des dispositions de la circulaire CSSF 22/806 en matière d'externalisation et en application du principe de proportionnalité (cf. paragraphe 3 de la présente circulaire), les établissements conservent en permanence une structure suffisante et adéquate permettant de garantir à tout moment la maîtrise de l'ensemble des activités de l'établissement.

Chapitre 2. Le dispositif de gouvernance interne

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

9. La gouvernance interne doit assurer la gestion saine et prudente des activités, y compris des risques qui leur sont inhérents. Le dispositif de gouvernance interne comprend notamment :

   - une structure organisationnelle et opérationnelle claire et cohérente comportant des pouvoirs de décision, des liens hiérarchiques et fonctionnels et un partage des responsabilités clairement définis, transparents, cohérents, complets et exempts de conflits d'intérêts ;
   - une structure organisationnelle claire en référence à la prestation des services de paiement et de monnaie électronique de l'établissement comprenant notamment le recours à des agents, des distributeurs, des bureaux de représentation ou des succursales ainsi que les politiques de l'établissement de sélection et de contrôle des agents, distributeurs, bureaux de représentation et succursales ;

- des mécanismes adéquats de contrôle interne qui répondent aux dispositions du chapitre 6 de cette partie. Ces mécanismes comprennent des procédures opérationnelles, administratives, comptables et informatiques saines et des politiques et pratiques de rémunération permettant et promouvant une gestion saine et efficace des risques, en ligne avec la stratégie de l'établissement en matière de risques, ainsi que des mécanismes de contrôle et de sécurité des systèmes d'information de gestion. La notion de système d'information de gestion comprend les systèmes informatiques ;
- une procédure formelle d'escalade, de règlement et, le cas échéant, de sanction pour les problèmes, déficiences et irrégularités relevés par le biais des mécanismes de contrôle interne, y compris les fonctions de contrôle interne, et par le biais des mécanismes d'alerte internes ;
- un processus clair de prise de risques comprenant un appétit au risque formellement et précisément arrêté dans tous les domaines d'activité et couvrant tous les types de risques auxquels l'établissement est exposé, y inclus les risques de blanchiment de capitaux et de financement de terrorisme, les risques opérationnels et de sécurité liés aux services de paiement ou de monnaie électronique qu'ils fournissent, ainsi qu'un processus décisionnel rigoureux, des analyses de qualité et des limites ;
- des processus de détection, de mesure, de déclaration, de gestion, d'atténuation et de contrôle appropriés en vue de gérer l'ensemble des risques auxquels l'établissement est ou pourrait être exposé, y inclus les risques de blanchiment de capitaux et de financement de terrorisme, les risques opérationnels et de sécurité liés aux services de paiement ou de monnaie électronique qu'ils fournissent ;
- un dispositif de communication interne 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 ;
- un dispositif de gestion de continuité des activités visant à limiter les risques de perturbation grave des activités et à assurer le maintien des activités essentielles telles que définies par l'organe de surveillance sur proposition de de l'organe de gestion. Ce dispositif comprend un plan de continuité qui décrit les actions à mettre en œuvre afin de poursuivre les activités en cas notamment d'incident, de sinistre ou de tout autre évènement susceptible de perturber les activités ainsi que des procédures efficaces de gestion des incidents, y compris pour la détection et la classification des incidents opérationnels et de sécurité majeurs ;
- un dispositif de gestion de crises qui assure une capacité de réaction appropriée en cas de crise.

10. Tout établissement promeut une culture interne de gestion des risques et de la conformité qui vise à assurer que tout le personnel de l'établissement participe activement au contrôle interne ainsi qu'à la détection, à la déclaration et au contrôle des risques encourus par l'établissement et adopte une attitude positive à l'égard du contrôle interne.

    Cette culture généralisée des risques et de la conformité, forte et omniprésente, doit également se refléter dans les stratégies, politiques et procédures de l'établissement, les formations proposées et les messages véhiculés aux membres du personnel en ce qui concerne la prise et la gestion des risques et la conformité au sein de l'établissement. Une telle culture se caractérise par l'exemple donné par les organes de surveillance et de gestion (« 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.

Cette culture généralisée des risques et de la conformité passe notamment par la communication régulière aux membres du personnel d'informations quant à l'appétit au risque de l'établissement, à la déontologie et aux valeurs d'entreprise de l'établissement dans la perspective d'un déploiement continu d'un robuste et efficace dispositif de contrôle interne.

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

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

- fonctionne de manière intègre (« intégrité »). Ce volet inclut aussi bien la gestion des conflits d'intérêts que la sécurité, en particulier en matière de systèmes d'information ;
- soit fiable et fonctionne de manière continue (« robustesse »). En vertu du principe de continuité, tout établissement se dote également d'arrangements visant à rétablir le fonctionnement du dispositif de gouvernance interne en cas de discontinuité ;
- soit efficace (« efficacité »). L'efficacité s'apprécie en particulier par rapport au fait que les risques sont effectivement gérés et contrôlés ;
- réponde aux besoins de l'établissement dans son ensemble et de toutes ses unités organisationnelles et opérationnelles (« adéquation ») ;
- soit cohérent dans son ensemble et dans ses parties (« cohérence ») ;
- soit complet (« exhaustivité »). En ce qui concerne les risques, l'exhaustivité signifie que l'ensemble des risques doit être inclus dans le périmètre du dispositif de gouvernance interne. Il doit permettre à l'établissement de disposer d'une vue exhaustive sur tous ses risques, en termes de substance économique, en tenant compte de toutes les interactions existant à travers l'établissement et de son réseau de distribution au travers d'agents, de distributeurs, de bureaux de représentation ou de succursales. S'agissant du contrôle interne, le principe d'exhaustivité implique que le contrôle interne porte sur tous les domaines de 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 l'organe de gestion et aux unités opérationnelles et organisationnelles de l'établissement ;
- soit conforme aux exigences légales et réglementaires, y compris par rapport aux exigences de la présente circulaire, aux exigences réglementaires applicables dans le domaine de la prévention du blanchiment et du financement du terrorisme (« conformité »).

12. 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 réévaluation objective, critique et régulière, au moins une fois par an par l'établissement (cf. également paragraphe 71 de la présente circulaire). Cette réévaluation 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.

Chapitre 4. L'organe de surveillance et l'organe de gestion

Sous-chapitre 4.1. L'organe de surveillance

Section 4.1.1. Responsabilités de l'organe de surveillance

13. L'organe de surveillance a la responsabilité globale de l'établissement. Il définit, surveille et porte la responsabilité de la mise en place d'un solide dispositif en matière d'administration centrale, de gouvernance, de contrôle interne et de gestion des risques, 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. À cette fin, l'organe de surveillance approuve et arrête par écrit, après avoir entendu l'organe de gestion et les responsables des fonctions de contrôle interne, les éléments clés suivants du dispositif en matière d'administration centrale, de gouvernance interne et de gestion des risques :

- la stratégie commerciale (modèle et plan d'affaires) de l'établissement dans le respect des intérêts financiers de l'établissement à long terme, de sa solvabilité, de la préservation de sa liquidité et de son appétit au risque. Le développement et le maintien d'un modèle d'affaires durable exigent la prise en compte de tous les risques matériels ;
- le programme d'activités ;
- la stratégie de l'établissement en matière de risques, y compris l'appétit au risque et le cadre global de prise et de gestion des risques de l'établissement y compris le cas échéant le risque de crédit et les limites en matière d'octroi de crédit en référence aux exigences de l'article 10, paragraphe 3, de la LSP ;
- les principes directeurs en matière de protection de fonds en référence aux exigences des articles 14 et 24-10 de la LSP ;
- les principes directeurs qui règlent la création et le maintien par l'établissement d'entités/structures juridiques telles que notamment les succursales, le réseau d'agents, de distributeurs et les bureaux de représentation ;
- les principes directeurs en matière de systèmes, de technologie et de sécurité de l'information ;

- les principes directeurs relatifs aux mécanismes de contrôle interne, qui incluent les fonctions de contrôle interne pour qu'ils soient efficaces et efficients ;
- les principes directeurs en matière de politique de rémunération ;
- les principes directeurs en matière de déontologie, de valeurs d'entreprise et de gestion des conflits d'intérêts ;
- les principes directeurs en matière d'escalade et de sanction visant à assurer que tout comportement non respectueux des règles applicables soit adéquatement poursuivi et sanctionné ;
- les principes directeurs en matière d'administration centrale au Luxembourg, comprenant :
    - les moyens humains et matériels que nécessite la mise en œuvre de la structure organisationnelle et opérationnelle ainsi que des stratégies de l'établissement,
    - une organisation opérationnelle, administrative, comptable et informatique intègre et respectant les lois et standards applicables,
    - les principes directeurs en matière d'externalisation (« outsourcing »), y compris de nature informatique reposant ou non sur une infrastructure de « cloud computing », ainsi que
    - les principes directeurs régissant la modification de l'activité (en termes de couverture de marchés et de clientèle, de nouveaux produits et de services) et l'approbation et le maintien d'activités inhabituelles ou potentiellement non transparentes ;
- les principes directeurs en matière de continuité des activités et de gestion de crises ;
- les principes directeurs régissant la nomination et la succession aux organes de surveillance et de gestion et aux fonctions de contrôle interne de l'établissement, ainsi que les procédures régissant l'organe de surveillance en termes de composition, comprenant les aspects de diversité, de responsabilités, d'organisation, de fonctionnement et d'évaluation individuelle et collective de ses membres ;
- la stratégie et les principes directeurs en matière de communication à l'égard de la clientèle et de marketing digital (cf. Internet, média sociaux, applications mobiles, etc.).

14. L'organe de surveillance charge l'organe de gestion de mettre en œuvre les stratégies et principes directeurs par le biais de politiques et de procédures internes écrites (à l'exception des principes directeurs qui régissent la nomination et la succession au sein de l'organe de surveillance et les procédures déterminant son fonctionnement).
15. L'organe de surveillance surveille la mise en œuvre par l'organe de gestion des stratégies et principes directeurs et en est informé. L'organe de surveillance prend, le cas échéant, connaissance des procédures et politiques que l'organe de gestion arrête en vertu de ces stratégies et principes.

16. L'organe de surveillance évalue d'une manière critique, adapte en cas de besoin et réapprouve à des intervalles réguliers, le dispositif de gouvernance interne, comprenant les stratégies clés et principes directeurs et leur mise en œuvre 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.

    Ces évaluations et leurs ré-approbations par l'organe de surveillance portent en particulier sur :

    - la manière dont l'organe de gestion s'acquitte 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 et informations fournies par l'organe de gestion et veille en particulier à ce que l'organe de gestion 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/ou toutes autorités compétentes ;
    - l'adéquation entre les risques encourus, la capacité de l'établissement à gérer ces risques compte tenu des stratégies et principes directeurs précédemment fixés par l'organe de surveillance et la réglementation applicable ;
    - 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 ;
    - l'adéquation de la structure organisationnelle et opérationnelle dont l'organe de surveillance doit avoir une compréhension parfaite. L'organe de surveillance veille à ce que la structure organisationnelle et opérationnelle permette à l'établissement de respecter ses stratégies et principes directeurs tout en maintenant une gestion saine et prudente des activités. L'organe de surveillance doit avoir une compréhension parfaite de la structure organisationnelle de l'établissement, en particulier en termes des entités ou structures juridiques sous-jacentes, de leur raison d'être, des liens et interactions intra-groupe qui les relient ainsi que des risques y liés. Il vérifie que la structure organisationnelle et opérationnelle correspond aux stratégies et principes directeurs, qu'elle permet une gestion saine et prudente des activités qui est exempte d'opacité et de complexité indue, et qu'elle reste justifiée par rapport aux objectifs assignés. Cette exigence s'applique tout particulièrement aux activités inhabituelles ou potentiellement non transparentes ;
    - l'efficacité et l'efficience des mécanismes de contrôle interne mis en place par l'organe de gestion.

    Les évaluations en question peuvent être préparées par des comités spécialisés. Elles se font notamment sur la base des informations reçues de la part de l'organe de gestion, des rapports de révision émis par le réviseur d'entreprises agréé (rapports sur les comptes annuels, comptes rendus analytiques et, le cas échéant, lettres de recommandations), des rapports financiers et des rapports des fonctions de contrôle interne que l'organe de surveillance est appelé à approuver.

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

18. S'agissant des fonctions de contrôle interne, l'organe de surveillance veille à ce que les travaux de ces fonctions soient exécutés suivant des normes reconnues et dans le cadre de politiques approuvées.

19. L'organe de surveillance veille à consacrer un temps suffisant aux thématiques du risque et de la conformité.

20. Lorsque l'organe de surveillance prend connaissance du fait que le dispositif en matière d'administration centrale ou de gouvernance interne ne permet plus une gestion saine et prudente des activités ou un respect des exigences en matière de protection des fonds définies aux articles 14 et 24-10 de la LSP ou que les risques encourus ne sont ou ne seront plus adéquatement supportés par la capacité de l'établissement à couvrir ces risques, par des fonds propres ou des réserves de liquidités internes, il exige de l'organe de gestion qu'il lui présente sans délai des mesures correctrices et en notifie immédiatement la CSSF. L'obligation de notification à la CSSF s'étend également à toutes les informations qui remettent en cause la qualification ou l'honorabilité d'un membre de l'organe de surveillance et/ou de gestion ou d'un responsable d'une fonction de contrôle interne.

Section 4.1.2. Composition et qualification de l'organe de surveillance

21. Les membres de l'organe de surveillance doivent être suffisants en nombre conformément aux dispositions légales applicables et présenter dans leur ensemble une composition adéquate qui permet à l'organe de surveillance de s'acquitter pleinement de toutes ses responsabilités et qui garantit une gestion saine et prudente de l'établissement. Le caractère adéquat se réfère en particulier aux qualités professionnelles (connaissances, compétences et expérience adéquates), ainsi qu'aux qualités personnelles des membres de l'organe de surveillance.

    Par ailleurs, chaque membre doit justifier en permanence de son honorabilité professionnelle.

    Les principes directeurs régissant la nomination et la succession des membres de l'organe de surveillance expliquent et arrêtent les facultés jugées nécessaires en vue d'assurer une composition et une qualification appropriées de l'organe de surveillance.

    La CSSF recommande que ces principes directeurs promeuvent les aspects de diversité. Les aspects de diversité peuvent faire référence aux caractéristiques des membres de l'organe de surveillance, y compris leur âge, genre, origine géographique et parcours éducatif et professionnel. La promotion de la diversité repose sur le principe de non-discrimination et sur des mesures garantissant l'égalité des chances.

22. L'organe de surveillance doit disposer collectivement de connaissances, compétences et d'expérience appropriées à la nature, à l'échelle et à la complexité des activités et de l'organisation de l'établissement.

L'organe de surveillance doit avoir collectivement une compréhension appropriée 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.

23. Les membres 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, disposent d'une compréhension appropriée des autres activités significatives de l'établissement et se tiennent informés des activités respectivement de l'évolution des activités de l'établissement et des risques auxquels l'établissement est exposé.

    Nonobstant les domaines d'expertise respectifs des membres de l'organe de surveillance, chaque membre de l'organe de surveillance doit disposer d'une compréhension appropriée de l'ensemble des domaines pour lesquels l'organe de surveillance est collectivement et directement responsable.

24. Les membres de l'organe de surveillance veillent à ce que leurs qualités personnelles leur permettent d'exécuter leur mandat de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit requis. 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 (membres de l'organe de gestion ou autres membres du personnel de l'établissement, à l'exception des représentants du personnel élus conformément à la réglementation applicable). La prise de décisions au sein de l'organe de surveillance ne doit pas être dominée par un seul membre.

25. Les membres de l'organe de surveillance veillent à ce que leur mandat soit et reste compatible avec leurs autres emplois, mandats et intérêts éventuels, en particulier en termes de conflits d'intérêts et de disponibilité. Ils informent de leur propre initiative l'organe de surveillance des emplois, mandats et intérêts éventuels qu'ils ont en dehors de l'établissement.

26. Les termes des mandats des membres de l'organe de surveillance doivent être fixés de manière à permettre à l'organe de surveillance d'exercer ses responsabilités de manière continue et efficace. La reconduction de membres existants doit s'orienter en particulier sur leurs performances passées. La continuité du fonctionnement de l'organe de surveillance doit être assurée.

27. Les principes directeurs régissant la nomination et la succession des membres de l'organe de surveillance prévoient les mesures nécessaires pour que ces membres soient et restent qualifiés tout au long de leur mandat et pour que le fonctionnement et la continuité de fonctionnement de l'organe de surveillance soient assurés. Ces mesures doivent inclure une initiation spécifique pour comprendre la structure, le modèle d'affaires, le profil de risque et le dispositif de gouvernance en vigueur au sein de l'établissement suivie par des programmes de formation professionnelle qui permettent aux membres de l'organe de surveillance de comprendre d'une part, leur rôle, les opérations de l'établissement, et d'autre part, de maintenir à jour et d'approfondir leurs compétences. Les mesures doivent également comprendre des durées de mandat différentes ou décalées ainsi que des dispositions contractuelles permettant d'assurer une transition efficace des connaissances et tâches d'un membre de l'organe de surveillance à son successeur ainsi que de respecter à tout moment le nombre minimal des membres de l'organe de surveillance conformément aux exigences légales applicables. Les mesures doivent également assurer une capacité de réaction appropriée en cas de crise.

28. Les établissements informent au préalable et sans délai la CSSF de toute modification de la composition des membres de l'organe de surveillance et communiquent pour chaque nomination, les informations et documents requis tels que publiés sur le site Internet de la CSSF, et pour les départs, les motifs explicatifs.

Section 4.1.3. Organisation et fonctionnement de l'organe de surveillance

29. 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. La CSSF recommande la tenue de réunions au minimum sur une base trimestrielle.

    En conformité avec les statuts de l'établissement et les exigences règlementaires applicables, les réunions de l'organe de surveillance peuvent se tenir en présentiel, par visioconférence ou par tout autre moyen de communication électronique permettant à l'ensemble de ses membres de suivre activement les discussions et d'y participer sans contrainte en temps réel. Sauf circonstances exceptionnelles, il est toutefois recommandé aux établissements d'assurer une majorité des réunions au siège de l'établissement au Luxembourg et en présence (sur place) d'une majorité de ses membres afin de stimuler la culture de discussion informée et contradictoire dans le cadre d'une prise de décision efficace.

30. Les travaux de l'organe de surveillance doivent être consignés par écrit. Cette documentation inclut l'agenda et les procès-verbaux des réunions avec les décisions et mesures prises par 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 également 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 en détail, permettant au lecteur de suivre les débats et d'identifier les positions défendues.

31. L'organe de surveillance évalue régulièrement les procédures régissant son mode de fonctionnement et ses travaux en vue de les améliorer, d'en assurer l'efficacité et de vérifier si les procédures qui lui sont applicables sont respectées dans la pratique. Il veille à ce que tous ses membres aient une vision claire de leurs obligations, de leurs responsabilités et de la répartition des tâches au sein de l'organe de surveillance et, le cas échéant, des comités spécialisés qui en dépendent.

32. L'organe de surveillance élit un président parmi ses membres. Il appartient au président de l'organe de surveillance de veiller à son bon fonctionnement, de promouvoir au sein de l'organe de surveillance une culture de discussion informée et contradictoire et de proposer, le cas échéant, la nomination d'un ou plusieurs membres indépendants. Le président de l'organe de surveillance n'assume pas de rôle exécutif au sein de l'établissement sauf lorsqu'une telle situation est justifiée par l'établissement et acceptée par la CSSF.

La présence d'un ou plusieurs membres indépendants au sein de l'organe de surveillance est recommandée et considérée comme une bonne pratique. Ces membres indépendants peuvent, en effet, jouer un rôle essentiel au sein de l'organe de surveillance et renforcer l'efficacité des contre-pouvoirs au sein de l'établissement en améliorant, le cas échéant, la surveillance de la prise de décisions par l'organe de surveillance.

Section 4.1.4. Comités spécialisés

33. En application du principe de proportionnalité (cf. paragraphe 3 de la présente circulaire), la CSSF pourra recommander à certains établissements de créer des comités spécialisés de l'organe de surveillance en fonction de leurs besoins et compte tenu de l'organisation, de la nature, de l'échelle et de la complexité des activités de l'établissement. Leurs missions consistent à fournir à l'organe de surveillance des appréciations critiques concernant l'organisation et le fonctionnement de l'établissement dans leurs domaines de compétences spécifiques.

34. 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. Chaque comité est composé d'au moins trois membres. Lorsqu'il existe au sein d'un établissement plusieurs comités spécialisés, l'établissement doit, dans la mesure où le nombre de membres non-exécutifs de l'organe de surveillance le permet, veiller à ce que les membres des comités respectifs soient différents. L'établissement doit par ailleurs essayer d'assurer une rotation des présidents et membres des comités spécialisés.

35. 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 informé et contradictoire au sein du comité.

36. Les comités spécialisés se réunissent régulièrement, afin d'exécuter les 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 membres de l'organe de gestion, 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.

37. L'organe de surveillance fixe par écrit la composition, les missions, 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. 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.

38. 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. L'organe de surveillance ne peut pas déléguer aux comités spécialisés ses pouvoirs et responsabilités en vertu de la présente circulaire.

Sous-chapitre 4.2. L'organe de gestion

Section 4.2.1. Responsabilités de l'organe de gestion

39. L'organe de gestion est responsable de la gestion journalière efficace, saine et prudente des activités et des risques qui leur sont inhérents. Les membres de l'organe de gestion sont responsables conjointement pour cette gestion qui s'exerce dans le respect des stratégies et principes directeurs approuvés par l'organe de surveillance et de la réglementation applicable, en prenant en considération et en préservant les intérêts financiers de l'établissement à long terme, sa solvabilité et ses liquidités. Cette gestion journalière couvre l'ensemble des fonctions, activités et risques de l'établissement.

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

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

42. En application des principes directeurs en matière de déontologie, de valeurs d'entreprise et de gestion des conflits d'intérêts arrêtés par l'organe de surveillance (cf. section 4.1.1. de la présente circulaire), l'organe de gestion définit un code de conduite interne applicable à tous les membres du personnel. Il veille à son application correcte sur la base de contrôles réguliers effectués par les fonctions de compliance et d'audit interne.

43. L'objectif de ce code de conduite doit être la prévention des risques opérationnels, de sécurité et de réputation dont l'établissement pourrait souffrir du fait d'amendes 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 des utilisateurs de services de paiement. Le code de conduite doit rappeler au personnel, aux membres de l'organe de gestion et de l'organe de surveillance le respect de la réglementation applicable, des règles internes, des principes sous tendant un comportement honnête et intègre en fournissant des exemples de comportements et de pratiques professionnelles acceptables et inacceptables ou interdites, y compris dans le domaine de la lutte contre le blanchiment et le financement du terrorisme, ainsi que les mesures de sanction qui découleraient du non-respect de ce cadre.

44. L'organe de gestion veille à ce que toutes les communications et marketing en particulier sous forme digitale (Internet, média sociaux, applications mobiles, etc.) soient conformes avec la stratégie de l'établissement et garantissent une communication claire, compréhensible, sans ambiguïté sur les services de paiement et/ou de monnaie électronique prestés par l'établissement et adapté dans son langage et sa forme à la clientèle visée par l'établissement. Il veille à la revue régulière de ces communications et marketing y inclus des informations publiées sur site Internet de l'établissement afin d'assurer l'utilisation d'un langage et d'une terminologie appropriée, sans ambiguïté et compréhensible par la clientèle visée par l'établissement en référence aux dispositions du présent paragraphe, du paragraphe 45 de la présente circulaire et en référence aux dispositions du titre III « Transparence des conditions et exigences en matière d'informations régissant les services de paiement » de la LSP.

45. L'organe de gestion veille à ce que l'utilisation de toute terminologie apparentée aux services réservés aux établissements de crédit tels que services bancaires, dépôts, banque ou néo-banque, compte bancaire, etc., ou à d'autres établissements (financiers) qui exercent des activités qui ne sont pas couvertes par les agréments d'établissement de paiement ou d'établissement de monnaie électronique, soit proscrite sous toutes ses formes.

46. L'organe de gestion met en œuvre de manière prompte et efficace les mesures correctrices pour remédier aux faiblesses (problèmes, déficiences, irrégularités ou préoccupations) relevées par les fonctions de contrôle interne et le réviseur d'entreprises agréé en prenant en compte les recommandations émises dans ce contexte. Cette manière de procéder est arrêtée dans une procédure écrite que l'organe de surveillance approuve sur proposition de l'organe de gestion et 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 l'organe de gestion, les délais appropriés endéans lesquels ces faiblesses seront corrigées. L'organe de gestion 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 la mise en œuvre des mesures correctrices liées au minimum à des faiblesses considérées par les fonctions de contrôle interne comme importantes, l'organe de gestion en informe l'organe de surveillance qui doit accepter les prolongations des délais de mise en œuvre des mesures correctrices.

47. L'établissement met en place une procédure analogue, approuvée par l'organe de surveillance, qui s'applique lorsque la CSSF ou toute autorité compétente demande à l'établissement de prendre des mesures (correctrices). Dans ce cas, tout retard dans la mise en œuvre de ces mesures est à signaler sans délai par l'organe de gestion à l'organe de surveillance et à la CSSF.

48. L'organe de gestion 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.

49. L'organe de gestion s'assure régulièrement de la solidité du dispositif en matière d'administration centrale et de gouvernance interne. Il adapte les politiques et procédures internes au regard des changements internes et externes, actuels et anticipés et des enseignements tirés du passé.

50. L'organe de gestion informe au préalable les fonctions de contrôle interne des changements majeurs en matière d'activités ou d'organisation afin de leur permettre de détecter et d'évaluer les risques qui peuvent en résulter. L'organe de gestion veille à ce que le dispositif de gouvernance y inclus le dispositif de contrôle interne reste, eu égard aux changements majeurs d'activités ou d'organisation, complet, fiable, efficace et transparent conformément aux paragraphes 9 et 11 de la présente circulaire.

51. Lorsque l'organe de gestion prend connaissance du fait que le dispositif en matière d'administration centrale et de gouvernance interne ne permet plus une gestion saine et prudente des activités ou un respect des exigences en matière de protection des fonds définies aux articles 14 et 24-10 de la LSP ou que les risques encourus ne sont ou ne seront plus adéquatement supportés par la capacité de l'établissement à couvrir ces risques par des fonds propres ou des réserves de liquidités internes, il en informe l'organe de surveillance et la CSSF en leur fournissant sans délai toute l'information nécessaire pour apprécier la situation et présente à l'organe de surveillance des mesures correctrices. L'obligation de notification à la CSSF porte aussi sur toutes les informations qui remettent en cause la qualification ou l'honorabilité d'un membre de l'organe de surveillance et/ou de gestion ou d'un responsable d'une fonction de contrôle interne.

52. L'organe de gestion désigne parmi ses membres la ou les personnes en charge des fonctions de contrôle interne et, conformément au Règlement CSSF N° 12-02, le responsable du respect des obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme. Les établissements informent au préalable la CSSF de toute modification de la composition des membres de l'organe de gestion, conformément aux dispositions légales y applicables et communiquent pour les nominations les documents requis tels que publiés sur le site Internet de la CSSF et/ou les motifs expliquant leur départ, le cas échéant.

53. En référence au paragraphe 11 de la présente circulaire, le dispositif en matière d'administration centrale et de gouvernance interne est élaboré et mis en œuvre de sorte notamment à ce qu'il fonctionne de manière continue. L'organe de gestion représente une fonction permanente essentielle du dispositif de gouvernance interne de l'établissement, il appartient ainsi à l'établissement et à ses organes de surveillance et de gestion d'assurer et de maintenir un dispositif de gouvernance interne conforme aux exigences légales et aux exigences de la présente circulaire et en particulier d'assurer, en cas de départ d'un membre de son organe de gestion, le maintien du principe des 4 yeux.

54. Il appartient à l'organe de gestion de promouvoir, avec l'organe de surveillance et les fonctions de contrôle interne, une culture interne en matière de gestion des risques et de conformité qui sensibilise le personnel de l'établissement aux impératifs d'une gestion saine et prudente des risques qui favorise une attitude positive à l'égard du contrôle interne et de la conformité et qui stimule le développement d'un dispositif de gouvernance interne qui permet d'atteindre ses objectifs.

Section 4.2.2. Composition et qualification de l'organe de gestion

55. Les membres de l'organe de gestion possèdent, à la fois individuellement et collectivement, les qualités professionnelles (connaissances, compétences et expérience appropriées à la nature, l'échelle et la complexité des activités et de l'organisation de l'établissement), l'honorabilité professionnelle et les qualités personnelles nécessaires pour gérer l'établissement et déterminer effectivement l'orientation de son activité. Les qualités personnelles sont celles qui leur permettent d'exécuter leur mandat de dirigeant de manière efficace, avec l'engagement, la disponibilité, l'objectivité, le sens critique et l'indépendance d'esprit requis.

    Les principes directeurs régissant la nomination et la succession à l'organe de gestion expliquent et arrêtent les facultés jugées nécessaires en vue d'assurer une composition et qualification appropriées de l'organe de gestion.

56. La CSSF recommande que ces principes directeurs régissant la nomination et la succession à l'organe de gestion promeuvent les aspects de diversité. Les aspects de diversité font référence aux caractéristiques des membres de l'organe de gestion, y compris leur âge, genre, origine géographique et parcours éducatif et professionnel. La promotion de la diversité repose sur le principe de non-discrimination et sur des mesures garantissant l'égalité des chances.

57. L'organe de gestion est composé à tout moment d'au moins deux personnes et ses membres doivent être habilités à déterminer effectivement l'orientation de l'activité. Le principe des 4 yeux doit être appliqué en toutes circonstances par l'organe de gestion. La composition de l'organe de gestion doit refléter le principe que cet organe travaille en collège. Chaque dirigeant doit être en mesure de démontrer sa capacité et son expérience à contribuer effectivement à ce collège dans divers aspects des activités à accomplir. Chaque dirigeant doit avoir une importance ou une influence significative dans la gestion journalière. Le lien hiérarchique entre les dirigeants (le cas échéant) ne peut pas empêcher la capacité de chaque dirigeant à s'opposer à une décision prise dans l'organe de gestion.

58. L'évaluation de la qualification des membres de l'organe de gestion est effectuée sur la base des conditions légales d'honorabilité et d'expérience professionnelles.

    À ce titre, le professionnel souhaitant devenir membre d'un organe de gestion d'un établissement doit être capable de démontrer l'adéquation de ses compétences avec les exigences légales par des expériences professionnelles antérieures similaires à un niveau élevé de responsabilité et d'autonomie.

    Il est attendu qu'un membre de l'organe de gestion jouisse d'une expérience et de connaissances suffisantes afin de lui permettre de gérer les activités quotidiennes dans le respect du cadre réglementaire applicable mais aussi des principes de gestion saine et prudente.

    Cette expérience s'apprécie tant par le niveau des responsabilités précédemment assumées que par la durée durant laquelle celles-ci ont été assumées, mais également par les qualifications acquises par le professionnel.

59. L'organe de gestion doit disposer collectivement de connaissances, compétences et d'une expérience appropriée à la nature, à l'échelle et à la complexité des activités et de l'organisation de l'établissement. Les membres de l'organe de gestion disposent individuellement d'une parfaite compréhension du dispositif de gouvernance interne et de leurs responsabilités au sein de l'établissement. Ils maîtrisent en particulier les activités et fonctions qui tombent sous leur responsabilité directe, disposent d'une compréhension et de connaissances appropriées des autres activités et domaines de responsabilité de l'établissement et se tiennent informés des activités respectivement de l'évolution des activités de l'établissement et des risques auxquels l'établissement est exposé.

    Nonobstant les domaines d'expertise respectifs des membres de l'organe de gestion, chaque membre de l'organe de gestion doit disposer d'une compréhension appropriée de l'ensemble des domaines pour lesquels l'organe de gestion est collectivement et directement responsable.

60. L'organe de gestion doit avoir une compréhension a de la structure organisationnelle et opérationnelle de l'établissement, en particulier en ce qui concerne son réseau de distribution, sa raison d'être et les risques y liés. Il 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 de son réseau de distribution.

61. Les termes des contrats des dirigeants doivent être fixés de manière à permettre à l'organe de gestion d'exercer ses responsabilités de manière continue et efficace.

62. Les principes directeurs régissant la nomination et la succession des membres de l'organe de gestion prévoient les mesures nécessaires pour que ces personnes soient et restent qualifiées tout au long de leur contrat et pour que le fonctionnement et la continuité de fonctionnement de l'organe de gestion soient assurées. Ces mesures doivent inclure une initiation spécifique pour comprendre la structure, le modèle d'affaires, le profil de risque et les dispositifs de gouvernance en vigueur au sein de l'établissement suivi par des programmes de formation professionnelle qui permettent aux membres de l'organe de gestion de comprendre d'une part, leur rôle, les opérations de l'établissement et d'autre part, de maintenir à jour et d'approfondir leurs compétences, y incluses leurs connaissances du cadre règlementaire applicable à l'établissement.

    Les mesures doivent permettre d'assurer une transition efficace des connaissances et tâches d'un membre de l'organe de gestion à son successeur ainsi que de respecter à tout moment le nombre minimal des membres de l'organe de gestion prévu par la présente circulaire. Les mesures doivent également assurer une capacité de réaction appropriée en cas de crise.

63. Les membres de l'organe de gestion veillent à ce que leurs responsabilités en tant que dirigeants soient et restent compatibles avec leurs autres mandats et intérêts éventuels, en particulier en termes de conflits d'intérêts, d'engagements et de disponibilités. Ils informent de leur propre initiative les autres membres de l'organe de gestion et l'organe de surveillance des mandats et intérêts éventuels qu'ils ont en dehors de l'établissement.

Section 4.2.3. Organisation et fonctionnement de l'organe de gestion

64. L'organe de gestion évalue de façon constructive et critique toutes les propositions, explications et informations qui lui sont soumises pour décision. L'organe de gestion 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 en détail, permettant au lecteur de suivre les débats et d'identifier les positions défendues.

65. Les membres de l'organe de gestion sont employés par l'établissement ou - à défaut - des dispositions contractuelles appropriées sont établies entre l'établissement et le membre concerné définissant notamment l'engagement et les conditions d'exercice du dirigeant en tant que membre de l'organe de gestion.

66. L'organe de gestion exerce une fonction permanente au sein de l'établissement. Sans préjudice des dispositions définies dans la circulaire CSSF 21/769 « Exigences en matière de gouvernance et de sécurité pour les entités surveillées en vue de l'exécution de tâches ou d'activités via le télétravail » telle que modifiée, ses membres doivent se trouver de façon permanente sur place.

67. La CSSF doit pouvoir contacter de façon directe au Luxembourg les membres de l'organe de gestion. Ces personnes doivent être en mesure de fournir, sans délai, sur toutes transactions ou opérations entreprises par l'établissement dans le cadre de ses activités, toutes les informations que la CSSF juge indispensables à sa surveillance, notamment celles sur la raison d'être et le but de ces transactions et/ou opérations.

68. Dans sa gestion journalière, l'organe de gestion tient compte des conseils et avis formulés par les fonctions de contrôle interne. Lorsque les décisions prises par l'organe de gestion ont ou pourraient avoir une incidence matérielle sur le profil de risque de l'établissement, l'organe de gestion recueille au préalable l'avis de la fonction compliance et, le cas échéant, de la fonction de contrôle des risques.

69. Les membres de l'organe de gestion se répartissent les tâches journalières du suivi rapproché des différentes activités. L'établissement doit organiser cette répartition de manière à éviter les conflits d'intérêts. Ainsi, un même membre de l'organe de gestion 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. 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.

70. L'organe de gestion informe, de manière adéquate, par écrit, régulièrement et au moins une fois par an, l'organe de surveillance sur la mise en œuvre, l'adéquation, l'efficacité et le respect du dispositif de gouvernance interne, comprenant l'état du contrôle interne. À cette occasion, il se prononce sur la réalisation des objectifs du contrôle interne, décrit les moyens mis en œuvre et présente un résumé des principales constatations faites, des insuffisances relevées, notamment par les fonctions de contrôle interne, des mesures correctrices décidées et du suivi effectif de ces mesures.

71. Une fois par an, l'organe de gestion confirme à la CSSF le respect de la présente circulaire par le biais d'une phrase écrite unique suivie des signatures de tous les membres de l'organe de gestion. Lorsqu'en raison d'un manque de conformité, l'organe de gestion n'est pas en mesure de confirmer le respect intégral de la présente circulaire, la déclaration précitée prend la forme d'une réserve qui énonce clairement et sommairement les points de non-conformité en donnant des explications sur leurs raisons d'être et les mesures décidées et/ou déjà prises pour remédier aux points de non-conformité.

    Cette attestation est à soumettre à la CSSF dans les meilleurs délais et au plus tard le dernier jour du troisième mois qui suit la date de clôture de l'exercice financier de l'établissement.

Chapitre 5. Organisation administrative, comptable et informatique

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

72. Conformément aux articles 11, paragraphe 2 et 24-7, paragraphe 2, de la LSP, les établissements doivent justifier d'une bonne organisation administrative et comptable ainsi que de procédures de contrôle interne adéquates.

73. L'établissement doit disposer sur place de ressources humaines suffisantes et disposant de compétences professionnelles individuelles et collectives appropriées afin d'agir et prendre des décisions dans le cadre des stratégies arrêtées par l'organe de surveillance et des politiques fixées par l'organe de gestion et conformément aux pouvoirs délégués, et afin d'exécuter les décisions prises dans le respect des procédures et de la réglementation existantes.

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

75. L'organigramme retient pour les différents services ou départements leur structure et les liens hiérarchiques et fonctionnels entre eux et avec l'organe de surveillance et l'organe de gestion.

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

77. L'organigramme et la description des tâches sont établis sur la 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 soient incompatibles dans le chef d'une même personne. Le but poursuivi est de prévenir au moyen d'un environnement de contrôles réciproques qu'une personne puisse commettre des erreurs et irrégularités qui ne seraient pas découvertes.

78. 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.

79. L'établissement dispose d'un programme de formation professionnelle continue qui assure que les membres du personnel, de l'organe de gestion et de l'organe de surveillance restent compétents et comprennent le dispositif de gouvernance interne ainsi que leurs propres rôles et responsabilités à cet égard.

80. Il est recommandé aux établissements d'établir une règle selon laquelle chaque membre du personnel prenne annuellement au moins deux semaines calendaires consécutives de congés personnels. Il doit être assuré que chaque membre du personnel soit effectivement absent pendant ce congé et que son remplaçant prenne effectivement en charge le travail de la personne absente.

Sous-chapitre 5.2. Les procédures et la documentation interne

81. Les établissements documentent par écrit l'ensemble du dispositif en matière d'administration centrale, de gouvernance interne y inclus de contrôle interne.

    Cette documentation porte sur les stratégies, les principes directeurs, les politiques et les procédures relatifs à l'administration centrale, à la gouvernance interne et à la gestion des risques. Elle comprend un manuel des procédures clair, complet, détaillé et accessible dont les procédures sont connues de l'ensemble du personnel concerné et qui est tenu à jour en continu.

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

    - les étapes successives et logiques du traitement des opérations, de leur initiation à l'archivage de leur documentation (« workflow »), incluant les seuils applicables, les flux de documents, le cas échéant, ainsi que la désignation des fonctions en charge de la réalisation de chacune des étapes ; et
    - les contrôles à réaliser, ainsi que les moyens pour s'assurer que ceux-ci ont été correctement réalisés et dans le respect des procédures applicables, incluant les seuils applicables, ainsi que la désignation des fonctions en charge des validations et contrôles de chacune des étapes.

83. 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 aux dispositions légales applicables. Elle doit être organisée de telle manière qu'elle puisse être aisément consultée par un tiers autorisé.

84. Comme le but est de garantir que les opérations sont exécutées de manière correcte, les procédures doivent être claires et complètes dans leur contenu et être connues par tous les membres du personnel concernés. Par ailleurs, les procédures doivent être mises à jour sans délai lors d'un changement interne ou externe ayant une incidence sur leur contenu.

85. Les dossiers, documents de travail et rapports de contrôle des fonctions de contrôle interne, des experts externes et des prestataires de services visés au sous-chapitre 6.2 relatif aux fonctions de contrôle interne ainsi que les rapports de révision établis par le réviseur d'entreprises agréé sont conservés pendant au moins cinq ans, sans préjudice d'autres législations applicables, dans l'établissement luxembourgeois afin de permettre à l'établissement de retracer les contrôles effectués, les problèmes, déficiences ou irrégularités relevés ainsi que les recommandations et conclusions. La CSSF et toute autorité compétente ainsi que le réviseur d'entreprises agréé doivent toujours pouvoir accéder à ces pièces.

86. Toutes les opérations initiées par l'établissement et les contacts avec les utilisateurs des services de paiement ou leurs mandataires émanent de l'établissement au Luxembourg. Toute la correspondance y est adressée et est expédiée à partir de l'établissement. 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 5.3. L'infrastructure administrative et technique

87. L'établissement se dote des fonctions de support et de contrôle, des moyens matériels et techniques nécessaires, suffisants et appropriés à l'exécution de ses activités et de la gestion des risques qui en découlent. Les moyens matériels et en particulier techniques doivent être adaptés à la nature, à l'échelle et à la complexité des activités de l'établissement ce qui inclut de permettre à l'établissement de minimiser les potentielles erreurs découlant de l'exécution de tâches manuelles.

Section 5.3.1. La fonction financière et comptable

88. L'établissement dispose d'une fonction financière et comptable dont la mission est d'assumer la gestion financière et comptable de l'établissement. Sans préjudice des exigences définies dans la circulaire CSSF 22/806 en matière d'externalisation de certaines tâches opérationnelles de la fonction financière et comptable, cette fonction financière et comptable doit veiller à ce que l'intervention d'autres services se fasse dans le strict respect du plan comptable et des instructions y relatives et sous le contrôle de la fonction comptable et financière.

89. La fonction financière et comptable fonctionnera suivant des règles et procédures écrites régulièrement revues et réévaluées et qui permettent :

- d'identifier et d'enregistrer toutes les transactions et opérations de paiement et de monnaie électronique entreprises par l'établissement ;
- d'expliquer l'évolution des soldes comptables d'un arrêté à l'autre par la conservation des mouvements ayant affecté les postes comptables ;
- d'établir les comptes par application des règles de comptabilisation et d'évaluation définies par la législation comptable et la réglementation y afférente ;
- de produire et de communiquer des informations périodiques et sur demande ponctuelle à la CSSF ou à tout autre autorité compétente ;
- de conserver toutes les pièces comptables suivant les dispositions légales en vigueur ;
- de s'assurer de la fiabilité et de la pertinence des prix et justes valeurs (« fair values ») utilisés dans l'établissement des comptes et du reporting à la CSSF ;

- de produire et de communiquer sans délai des informations périodiques et ponctuelles à la CSSF, comprenant en premier lieu le reporting légal et réglementaire, et d'en assurer la fiabilité, notamment en matière de solvabilité et de protection des fonds des utilisateurs de service de paiement ; dans ce contexte, les établissements sont tenus de disposer à la fin de chaque jour, sans condition et ou restriction d'accès de quelque nature que ce soit, des balances de tous les comptes et de tous les mouvements comptables de la journée afin de fournir sans délai à toute autorité compétente les informations requises ;
- d'établir, le cas échéant, des comptes suivant le schéma comptable en vigueur dans le pays d'origine de l'actionnaire en vue de l'établissement des comptes consolidés ;
- de réaliser les réconciliations des comptes et des écritures comptables ;
- de produire une information financière fiable et rapidement disponible à l'organe de gestion (« management information ») et à l'organe de surveillance afin de leur permettre de suivre de près l'évolution de la situation financière y inclus la solvabilité de l'établissement et sa conformité aux données budgétaires. Cette information servira comme instrument de contrôle de gestion et sera d'autant plus efficace si elle est basée sur une comptabilité analytique ;
- de s'assurer de la fiabilité du reporting financier.

90. Sans préjudice des contrôles déployés au niveau de la fonction financière et comptable ou d'externalisation de certaines tâches de la fonction financière et comptable, les informations à communiquer périodiquement et ponctuellement sur demande de la CSSF et de toute autorité compétente doivent être systématiquement et formellement revues et validées par un membre de l'organe de gestion.

91. En application du principe de proportionnalité, la CSSF pourra recommander à certains établissements de se doter d'un responsable dédié à la fonction financière et comptable et au contrôle de gestion. Ce responsable rapporte directement à l'organe de gestion.

    Ce responsable dédié à la fonction financière et comptable et au contrôle de gestion doit posséder des connaissances et compétences appropriées et une expérience professionnelles élevées dans le domaine comptable et financier y inclus en ce qui concerne les normes comptables applicables. Il est recommandé que cette personne soit sélectionnée, nommée et révoquée suivant une procédure interne écrite, avec approbation au préalable par l'organe de surveillance.

92. Les tâches exercées au sein de la fonction financière et comptable ne peuvent pas être cumulées avec d'autres tâches incompatibles, tant commerciales qu'administratives.

93. Dans le cadre de l'ouverture de comptes de contreparties/comptes de tiers, chaque établissement définit des règles précises d'enregistrement des comptes dans sa comptabilité. Il précise par ailleurs les conditions auxquelles l'autorisation est donnée afin que ces comptes fonctionnent et auxquelles ils peuvent être clôturés.

94. 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. À cet effet, l'établissement mettra en place des procédures de vérification et de suivi appropriées.

95. L'ouverture et la clôture des comptes internes dans la comptabilité doivent être validées par la fonction financière et comptable. En cas d'ouverture des comptes, cette validation doit intervenir avant que ces comptes ne commencent à devenir opérationnels. L'établissement fixe des règles concernant l'utilisation de tels comptes et les pouvoirs pour leur ouverture. La fonction financière et comptable 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.

96. 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 la fonction financière et comptable.

97. L'ensemble de l'organisation et des procédures comptables est décrit dans un manuel ou livre des procédures comptables.

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

Section 5.3.2. La fonction informatique

98. 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. Pour ce faire, ils respectent les exigences du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier et des circulaires CSSF relatives aux exigences en matière de gestion des risques liés aux TIC et à la sécurité. Ils maintiennent également à jour les informations et documents tels que demandés dans la circulaire CSSF 18/677 relative aux Orientations de l'Autorité bancaire européenne sur les informations à fournir dans le cadre de l'agrément d'établissements de paiement et d'établissements de monnaie électronique et pour l'enregistrement de prestataires de services d'information sur les comptes au titre de l'article 5, paragraphe 5, de la directive (UE) 2015/2366 (EBA/GL/2017/09).

99. Les établissements qui, en matière de fonction informatique, recourent aux services de prestataires de services doivent se référer à la circulaire CSSF 22/806 concernant l'externalisation.

Section 5.3.3. Le dispositif de communication et d'alerte interne et externe

100. Le dispositif de communication interne assure que les stratégies, politiques et procédures de l'établissement ainsi que les décisions et mesures prises par l'organe de gestion, 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.

101. 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 délai à tous les membres de l'organe de gestion, à l'organe de surveillance et au 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.

102. La loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union a pour objet de protéger l'auteur d'un signalement de violations contre les représailles de la part d'un employeur ou d'une autre personne physique ou morale exerçant un certain pouvoir de contrainte en rapport avec l'activité du « lanceur d'alerte ». Cette obligation s'applique à toutes les entités juridiques de droit privé. La CSSF met également à disposition sur son site Internet un outil et une procédure permettant la déclaration de tels signalements directement à la CSSF (procédure de signalement externe) (https://whistleblowing.apps.cssf.lu/ index.html?language=fr). Le dispositif légal applicable est complété par l'article 8-3 de la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et le financement du terrorisme, tel qu'introduit par la loi du 25 mars 2020, prévoyant un cadre spécifique de signalement en matière de LBC/FT et par l'article 58-10 de la loi du 10 novembre 2009 relative aux services de paiement, tel que modifié, qui permet à la CSSF de mettre en place des mécanismes efficaces favorisant la déclaration des violations du Règlement (UE) 2015/847.

Chapitre 6. Le contrôle interne

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

    Les mécanismes de contrôle interne doivent également être appliqués par les succursales que les établissements ont à l'étranger sans préjudice de dispositions légales ou règlementaires locales qui existent en la matière.

    Le dispositif de contrôle interne doit comprendre des processus et procédures efficaces prévenant la fraude et assurant tant le respect des obligations en matière de lutte contre le blanchiment et le financement du terrorisme que le respect des obligations visant à prévenir, rechercher, détecter et le cas échéant rapporter des fraudes en matière de paiements. Les établissements doivent évaluer leur exposition au risque d'être abusés notamment à des fins de blanchiment ou de financement du terrorisme, adapter leur dispositif de contrôle au niveau du risque identifié (approche basée sur le risque) et prendre des mesures efficaces d'atténuation visant à réduire ce risque, ainsi que les risques opérationnels et de réputation associés. Le dispositif garantit l'information et la formation adéquate du personnel par rapport à ces risques.

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

- la première ligne de défense est constituée par les unités opérationnelles qui prennent ou acquièrent des risques, qui assument la responsabilité pour leur gestion et qui contrôlent de manière permanente le respect des politiques, procédures et limites qui leur sont imposées ;
- la seconde ligne est formée par des fonctions de support, comme la fonction financière et comptable, mais surtout la fonction compliance et la fonction de contrôle des risques (dans la mesure où celle-ci est prévue en vertu du paragraphe 163 de la présente circulaire), qui assurent un contrôle indépendant des risques et supportent les unités opérationnelles dans le respect des politiques et procédures qui leur sont applicables ;
- la troisième ligne est constituée par la fonction d'audit interne qui effectue une évaluation indépendante, objective et critique des deux premières lignes de défense et du dispositif de gouvernance interne dans son ensemble.

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

105. 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.

106. Les contrôles réalisés (c.-à-d. contrôles opérationnels, contrôle des risques, etc.) doivent être suffisamment et précisément documentés afin de permettre de démontrer leur exécution et leur efficacité.

Sous-chapitre 6.1. Les contrôles opérationnels

Un environnement de contrôle interne robuste et solide comporte notamment les types de contrôles suivants qui relèvent de la première ligne de défense :

Section 6.1.1. Les contrôles quotidiens réalisés par le personnel exécutant

107. Les procédures en matière de contrôle interne prévoient que les exécutants contrôlent sur une base quotidienne les tâches opérationnelles et/ou processus qu'ils exécutent dans le cadre des activités de l'établissement ou des services prestés par l'établissement, ceci afin de détecter le plus rapidement possible des erreurs et omissions survenues dans le traitement de ces tâches opérationnelles et processus courants. Lorsque ces tâches opérationnelles sont externalisées, l'établissement doit s'assurer qu'elles sont exécutées correctement et en conformité avec la circulaire CSSF 22/806 relative à l'externalisation.

Section 6.1.2. Les contrôles critiques continus

108. Dans cette catégorie de contrôles tombent notamment :

- le contrôle hiérarchique ;
- la validation (par exemple la double signature, les codes d'accès à des fonctionnalités données) associée au contrôle du respect de la procédure d'autorisation et de délégation de pouvoirs arrêtée par l'organe de gestion ;
- les contrôles réciproques ;
- le relevé régulier de l'existence et de la valeur des éléments du patrimoine et des fonds des utilisateurs de services de paiement, notamment au moyen de la vérification des inventaires ;
- la réconciliation et la confirmation des comptes ;
- le contrôle de l'exactitude et de l'exhaustivité des données communiquées par les personnes en charge des fonctions commerciales et opérationnelles en vue d'un suivi administratif des opérations ;
- la vérification du 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 éventuels.

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

Section 6.1.3. Les contrôles réalisés par les membres de l'organe de gestion sur les activités ou fonctions qui tombent sous leur responsabilité directe

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

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

- les risques liés aux activités et fonctions dont ils sont directement responsables ;
- le respect des lois et normes applicables à l'établissement, avec une attention particulière pour les exigences à respecter en termes de protection des fonds reçus des utilisateurs des services de paiement ;
- le respect des politiques et procédures arrêtées par l'organe de gestion et l'organe de surveillance ;
- le respect des budgets établis et l'examen des réalisations effectives et des écarts ;
- le respect des limites (notamment sur la base de rapports d'exception) ;
- les caractéristiques des opérations, notamment leur prix, leur rentabilité individuelle ;

- l'évolution de la rentabilité globale d'une activité.

111. Les membres de l'organe de gestion informent régulièrement les autres membres de l'organe de gestion sur l'exercice de leur mission de contrôle lors des réunions de l'organe de gestion.

112. Le dispositif de contrôle interne prévoit une documentation appropriée par écrit des différents niveaux de contrôle tels que décrits ci-avant permettant de rendre compte de la mise en œuvre effective des politiques et procédures internes. Cette documentation inclut tant les contrôles manuels et hiérarchiques opérés par les différents niveaux de contrôle que les contrôles automatisés et/ou intégrés dans les systèmes de paiement ou autres outils utilisés par l'établissement.

Sous-chapitre 6. Les fonctions de contrôle interne

113. Les politiques mises en œuvre en matière de conformité et d'audit interne instaurent deux fonctions de contrôle interne distinctes : d'une part, la fonction compliance qui relève de la deuxième ligne de défense et d'autre part, la fonction d'audit interne qui relève de la troisième ligne de défense.

    Lorsque l'établissement se dote d'une fonction indépendante et permanente de contrôle des risques, elle relève également de la seconde ligne de défense.

    Les politiques de l'établissement 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.

    Les sections 6.2.1., 6.2.2., 6.2.3. et 6.2.4. de la présente circulaire et relatives aux responsabilités génériques, aux caractéristiques, à l'exécution des travaux et à l'organisation des fonctions de contrôle interne s'appliquent à la fonction de compliance et à la fonction d'audit interne.

    Lorsque l'établissement se dote ou est tenu de se doter d'une fonction indépendante et permanente de contrôle des risques conformément au principe de proportionnalité établi aux paragraphes 3 et 162 de la présente circulaire, les sections 6.2.1., 6.2.2., 6.2.3. et 6.2.4. de la présente s'appliquent à cette fonction.

Section 6.2.1. Responsabilités génériques des fonctions de contrôle interne

114. 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 l'organe de gestion ainsi qu'à l'organe de surveillance et, le cas échéant, aux comités spécialisés. Elles fournissent à l'organe de gestion ainsi qu'à l'organe de surveillance et, le cas échéant, aux comités spécialisés les avis et conseils qu'elles jugent utiles ou qui leur sont demandés par ces organes ou comités. Nonobstant les responsabilités spécifiques en la matière attribuées à la fonction compliance, toutes les fonctions de contrôle interne contribuent à la lutte efficace contre le blanchiment et le financement du terrorisme.

115. 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 l'organe de gestion et l'organe de surveillance et les comités spécialisés, le cas échéant.

Section 6.2.2. Caractéristiques des fonctions de contrôle interne

116. 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 à l'organe de surveillance ou à son président, et, le cas échéant, aux comités spécialisés qui en émanent, au réviseur d'entreprises agréé de l'établissement ainsi qu'à la CSSF.

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

- le personnel des fonctions de contrôle interne est chargé de tâches qu'il est appelé à contrôler ;
- la rémunération du personnel des fonctions de contrôle interne est liée à la performance des activités qu'elles contrôlent ou déterminée suivant d'autres critères qui compromettent l'objectivité du travail accompli par les fonctions de contrôle interne ;
- les fonctions de contrôle interne sont intégrées d'un point de vue organisationnel dans les unités opérationnelles qu'elles contrôlent ou dépendent hiérarchiquement d'elles ;
- les responsables des fonctions de contrôle interne sont subordonnés aux personnes en charge de, ou responsables pour, les activités que les fonctions de contrôle internes sont appelées à contrôler. Dans le cadre d'un établissement ne possédant que deux dirigeants, l'application du principe de proportionnalité imposera la séparation de la supervision des fonctions de contrôle interne de seconde et troisième ligne.

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

119. Les fonctions de contrôle interne ou les prestataires de services agissant pour le compte de ces fonctions doivent effectuer leurs travaux avec objectivité.

    Afin de garantir leur objectivité, les personnes relevant des fonctions de contrôle interne possèdent l'indépendance d'esprit ; elles ne doivent pas subordonner leur propre jugement à celui d'autres personnes, dont surtout les personnes contrôlées, et veillent à éviter les conflits d'intérêts.

120. Les principes directeurs régissant la nomination et la succession des responsables de fonctions de contrôle interne prévoient les mesures nécessaires pour que ces membres soient et restent qualifiés. Ces mesures doivent inclure une initiation spécifique pour comprendre la structure, le modèle d'affaires, le profil de risque et les dispositifs de gouvernance et ensuite des programmes de formation professionnelle qui permettent aux responsables des fonctions de contrôle interne 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. Les mesures doivent également assurer à tout moment la permanence des responsables des fonctions de compliance et d'audit interne et le cas échéant de contrôle des risques. Ces mesures doivent également assurer une capacité de réaction appropriée en cas de crise.

121. Les membres des fonctions de contrôle interne doivent posséder un niveau individuel et collectif élevé de connaissances, de compétences et une expérience professionnelle dans le domaine des activités de paiement et/ou de monnaie électronique ou similaires et plus particulièrement dans leur domaine de responsabilités en ce qui concerne les normes applicables. Conformément au principe de proportionnalité, le niveau de compétences requis augmente en fonction de l'organisation de l'établissement et de la nature, de l'échelle et de la complexité des activités et des risques. La compétence individuelle doit comporter la capacité de porter des jugements critiques et d'être écouté par les membres de l'organe de gestion de l'établissement.

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

123. En sus de leur expérience professionnelle élevée, les responsables de fonctions de contrôle interne qui accèdent pour la première fois à une telle position possèdent les connaissances théoriques nécessaires.

124. Pour garantir l'exécution des tâches qui leur incombent, les fonctions de contrôle interne disposent des ressources humaines, de l'infrastructure et des budgets nécessaires et suffisants, conformément au principe de proportionnalité. Le budget doit être suffisamment flexible pour tenir compte d'une adaptation des missions des fonctions de contrôle interne en réponse à des changements au niveau de l'organisation, des activités et des risques de l'établissement ou en cas de survenance d'événements spécifiques. Les établissements qui, en matière de fonctions de contrôle interne, recourent aux services de prestataires de services doivent se référer à la circulaire CSSF 22/806 concernant l'externalisation.

125. Le champ d'intervention des fonctions de contrôle interne couvre l'ensemble de l'établissement, y inclus les succursales, dans le respect de leurs compétences respectives. Il inclut les activités menées à travers des réseaux d'agents, de distributeurs ou de bureaux de représentation ainsi que les activités inhabituelles et potentiellement non transparentes.

126. 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

127. 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.

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

129. 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 l'organe de gestion, des problèmes (existants ou émergents), déficiences et irrégularités majeurs survenus depuis le dernier rapport, des mesures prises pour y remédier ainsi qu'une description des contrôles réalisés, des insuffisances et anomalies constatées, mais également des recommandations et des propositions sur les mesures correctrices à prendre, de même qu'une prise de position des personnes contrôlées assortie d'un délai approprié pour la mise en place d'actions correctrices, le cas échéant. Une indication de l'importance relative des anomalies et déficiences en fonction de leur niveau de risque et de priorité est fourni.

130. Le rapport de synthèse des fonctions de contrôle interne fournit un état des lieux portant sur l'accomplissement du plan de contrôle tel qu'il avait été défini pour l'année. Il inclut également, le cas échéant, la justification des retards ou reports de mission.

131. Le rapport de synthèse des fonctions de contrôle interne dresse un inventaire des contrôles clés effectués par thématique couverte, et inclut une description de ces contrôles (recours à un test de cheminement, échantillonnage, revue des procédures etc.).

132. Le rapport de synthèse des fonctions de contrôle interne doit à la fois faire état des exceptions identifiées pour lesquelles des actions de remédiation n'ont pas encore été mises en œuvre, mais aussi de celles qui ont d'ores et déjà été considérées comme clôturées au cours de l'année.

133. Le rapport de synthèse des fonctions de contrôle interne comprend une section dédiée au suivi des exceptions identifiées au cours des années précédentes mais non encore clôturées à la date de remise du précédent rapport, incluant une mise à jour quant à la façon dont les exceptions ont été clôturées, ainsi qu'une prise de position de l'organe de gestion ainsi que de nouveaux délais, le cas échéant.

134. Enfin, le rapport de synthèse des fonctions de contrôle interne se prononce sur l'état de leur domaine de contrôle dans son ensemble. S'agissant du fonctionnement, le rapport se prononce en particulier sur l'adéquation des ressources humaines et techniques internes et la nature et le degré du recours à des ressources humaines et techniques externes ainsi que sur les problèmes éventuels apparus dans ce contexte. Ce rapport est soumis pour approbation à l'organe de surveillance ou, le cas échéant, aux comités spécialisés compétents pour en assurer le suivi avec l'organe de surveillance ; il est soumis pour information à l'organe de gestion. Ce rapport est à rédiger en français, allemand ou anglais.

135. En cas de problèmes, déficiences et irrégularités graves, les responsables des fonctions de contrôle interne en informent immédiatement l'organe de gestion, le président de l'organe de surveillance et les présidents des comités spécialisés, le cas échéant. Dans ces cas, les responsables des fonctions de contrôle interne peuvent demander à être entendus par l'organe de surveillance en séance privée.

136. 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 paragraphe 46 de la présente circulaire. Elles rapportent de manière régulière à ce sujet à l'organe de gestion. Pour tout retard dans la mise en œuvre des mesures correctrices, l'organe de gestion en informe l'organe de surveillance qui doit autoriser les prolongations des délais de mise en œuvre des mesures correctrices.

Section 6.2.4. Organisation des fonctions de contrôle interne

137. Chaque fonction de contrôle interne est placée sous la responsabilité d'un chef de fonction distinct qui est sélectionné, nommé et révoqué par l'organe de gestion suivant une procédure interne écrite. Il est recommandé de faire approuver les nominations et révocations des responsables des fonctions de contrôle interne au préalable par l'organe de surveillance.

138. Les établissements informent au préalable par écrit et sans délai la CSSF de toute modification du « Chief Internal Auditor » et du « Chief Compliance Officer » et fournissent pour chaque nomination, les informations et documents requis tels que publiés sur le site Internet de la CSSF et pour les départs, les motifs explicatifs. Lorsque l'établissement se dote d'une fonction indépendante et permanente de contrôle des risques, l'établissement communique par écrit à la CSSF le nom du responsable de cette fonction et informe sans délai la CSSF de tout changement concernant le responsable de cette fonction.

139. Les responsables des fonctions de contrôle interne sont responsables vis-à-vis de l'organe de gestion et, en dernier ressort, vis-à-vis de l'organe de surveillance pour l'exécution de leur fonction. À ce titre, ces responsables doivent pouvoir contacter directement et de leur propre initiative l'organe de surveillance ou son président, et le cas échéant, le comité spécialisé compétent.

140. Les responsables des fonctions de contrôle interne sont désignés par « Chief Compliance Officer » pour la fonction compliance et « Chief Internal Auditor » pour la fonction d'audit interne. Au cas où une fonction de contrôle des risques indépendante est établie, le responsable de cette fonction est désigné par « Chief Risk Officer ».

141. Une éventuelle externalisation de tâches opérationnelles d'une fonction de contrôle interne n'est admise qu'en conformité avec la circulaire CSSF 22/806 applicable en matière d'externalisation.

142. Tout recours à des prestataires de services, doit se faire en conformité avec les exigences de la circulaire CSSF 22/806 concernant l'externalisation. Ces prestataires réalisent leurs travaux dans le respect des dispositions réglementaires et internes qui sont applicables à la fonction de contrôle interne et au domaine de contrôle en question. Elles doivent être placées sous la dépendance du responsable de la fonction de contrôle interne. Ce responsable supervise les travaux de ces prestataires externes.

143. Les fonctions de contrôle interne du siège de l'établissement procèdent régulièrement à des contrôles sur place auprès des succursales. Lorsque l'établissement a une succursale d'une certaine taille conformément au principe de proportionnalité, les fonctions de contrôle interne d'un établissement doivent également être mises en place au niveau de cette succursale.

144. Les fonctions de contrôle interne des succursales dépendent, d'un point de vue hiérarchique et fonctionnel, des fonctions de contrôle des entités juridiques dont elles font partie et auxquelles elles rapportent. Les responsables des fonctions de contrôle de l'établissement donnent leur accord pour tout recrutement, licenciement des chefs des fonctions de contrôle des succursales. Les rapports établis conformément aux dispositions de la présente circulaire sont soumis non seulement au responsable local de la succursale, mais également aux fonctions de contrôle interne de l'établissement.

Section 6.2.5. La fonction compliance

Sous-section 6.2.5.1. La charte de compliance

145. 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 l'organe de gestion et par l'organe de surveillance en dernier ressort.

146. La charte 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, bureaux de représentation et agents ou distributeurs 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 objectifs, responsabilités, compétences et lignes de reporting de la fonction de compliance ;
- décrire les relations avec les fonctions d'audit interne et le cas échéant de contrôle des risques ainsi que d'éventuels besoins de délégation au sein de l'établissement 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 de l'organe de surveillance ou, le cas échéant, les membres des comités spécialisés, ainsi que la CSSF.

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

147. La charte de compliance doit être évolutive et mise à jour dans les meilleurs délais pour tenir compte des changements au niveau des normes en vigueur affectant l'établissement. Toutes les modifications doivent être approuvées par l'organe de gestion et par l'organe de surveillance.

Sous-section 6.2.5.2. Champ d'application et responsabilités spécifiques de la fonction compliance

148. La fonction compliance a pour objectif d'anticiper, de détecter, d'évaluer, de déclarer et de suivre les risques de non-conformité d'un établissement ainsi que d'assister les organes de gestion et de surveillance à doter l'établissement de mesures pour se conformer aux lois, règlements et standards applicables. Les risques de non-conformité 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.

Les tâches de la fonction compliance sont à réaliser continuellement et sans délai.

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

- la fonction compliance identifie, de manière continue, 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.

  Par « normes », il faut entendre dans ce contexte toutes les règles auxquelles l'établissement est soumis dans l'exercice de ses activités dans ses différents marchés ;
- la fonction compliance identifie les risques de non-conformité 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 non-conformité 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 non-conformité avant que l'établissement ne se lance dans un nouveau type d'activité, de produit ou de relation d'affaires, de marchés, de même que lors du développement des opérations et du réseau d'un groupe sur une échelle internationale (« New Product Approval Process », tel que défini au sous-chapitre 7.3. de la présente circulaire) ;

- la fonction compliance veille à ce que, pour la mise en œuvre de la politique de conformité, l'établissement dispose de règles qui puissent servir de lignes directrices au personnel des différents métiers dans l'exercice de leurs tâches journalières. Ces règles doivent être reflétées de façon appropriée dans les instructions, procédures et contrôles internes pour les domaines relevant directement de la fonction compliance et tiennent compte du code de conduite et des valeurs d'entreprise dont s'est doté l'établissement.

  Pour les établissements disposant de succursales, la politique de conformité au niveau de ces succursales doit tenir compte des normes applicables au niveau local ;

- les domaines qui relèvent directement de la fonction compliance sont typiquement la lutte contre le blanchiment de capitaux et le financement du terrorisme, les fraudes, la protection des intérêts et des données des utilisateurs des services de paiement ainsi que la protection de leurs fonds et la prévention et la gestion des conflits d'intérêts. Cette liste n'est pas exhaustive et il appartient à l'établissement de décider si sa fonction compliance couvre également le respect d'autres règles que celles énoncées ci-avant ;

- en tant que responsable du contrôle des obligations professionnelles en matière LBC/FT, 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 aux risques.

  Le rapport de synthèse de la fonction compliance adressé en copie à la CSSF couvrira tous les domaines qui relèvent de la fonction compliance, relatant de manière concise mais sans omission 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. Le rapport rendra compte de l'état d'avancement du plan de surveillance de la conformité (« compliance monitoring plan ») et en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, notamment les contrôles prévus à effectuer par la fonction compliance, et expliquera les éléments du plan n'ayant pas pu être achevés dans les délais prévus. Le rapport doit permettre d'évaluer la gravité des événements couverts et l'adéquation du plan de surveillance de la conformité, afin de rendre possible un jugement global sur l'adéquation et le fonctionnement efficace du cadre préventif mis en place par l'établissement ;

- d'une manière générale, la fonction compliance est à organiser de façon à couvrir tous les domaines pouvant donner lieu à des risques de non-conformité. Il est admissible que les domaines autres que ceux énumérés ci-dessus ne soient pas directement couverts par la fonction compliance. Le risque de non-conformité est alors à couvrir par les autres fonctions de contrôle interne suivant une politique de conformité 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.

150. La fonction compliance procède régulièrement à une vérification du respect de la politique de conformité et des procédures et se charge, en cas de besoin, des propositions d'adaptation. À cette fin, la fonction compliance effectue des évaluations et des contrôles réguliers du risque de non-conformité dans le cadre d'un programme de contrôle structuré. Pour les contrôles en matière de risque de non-conformité 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.

151. La fonction compliance centralise toutes les informations sur les problèmes de non-conformité (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 l'organe de gestion ou, le cas échéant, de l'organe de surveillance) ou externes (par exemple rapports du réviseur d'entreprises agréé, correspondance de la part des autorités compétentes).

152. La fonction compliance assiste et conseille l'organe de gestion pour des questions de conformité et de lois, règlements et standards applicables, notamment en le rendant attentif à des développements au niveau des normes qui pourraient ultérieurement avoir un impact sur le domaine de la compliance.

153. La fonction compliance veille à sensibiliser le personnel à l'importance de la conformité 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.

154. Le « Chief Compliance Officer » est la personne de contact privilégiée des autorités compétentes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme pour toute question relative à ce domaine. Il est également chargé de la transmission de toute information ou déclaration auprès desdites autorités.

Sous-section 6.2.5.3. Organisation de la fonction compliance

155. Les établissements créent une fonction compliance permanente et indépendante compte tenu des considérations générales sur l'organisation des fonctions de contrôle interne et des caractéristiques des fonctions de contrôle interne élaborées aux précédentes sections.

156. Le « Chief Compliance Officer » est employé à plein temps par l'établissement à Luxembourg, et est dédié à 100% à la fonction compliance. Il n'est pas admis de cumuler les responsabilités de « Chief Compliance Officer » et de contrôle des risques dans le chef d'une seule personne ou de combiner la responsabilité de « Chief Compliance Officer » avec d'autres tâches incompatibles avec ses responsabilités.

A titre exceptionnel, en référence au principe de proportionnalité, l'établissement qui envisage le maintien d'un « Chief Compliance Officer » à temps partiel ou partiellement dédié à la fonction compliance (ex. attribution de tâches de contrôle des risques au « Chief Compliance Officer »), doit adresser une demande écrite à la CSSF qui comprendra :

- une description de l'organisation de la fonction de compliance ;

- l'analyse et ses conclusions justifiant que la fonction de compliance dispose au Luxembourg des ressources humaines, de l'infrastructure et des budgets nécessaires et suffisants afin d'assumer ses tâches et responsabilités en conformité avec les principes de la présente circulaire et de sorte que les risques de non-conformité, et en particulier les risques liés au blanchiment d'argent et au financement du terrorisme, sont atténués de façon appropriée et dans les limites de l'appétit au risque approuvé par l'organe de surveillance;
- la décision de l'organe de gestion et de l'organe de surveillance approuvant l'analyse et ses conclusions.

157. Sans préjudice des exigences définies dans de la circulaire CSSF 22/806 en matière d'externalisation en particulier en relation avec l'externalisation de certaines tâches opérationnelles de la fonction compliance ou avec le recours ponctuel à l'expertise ou aux moyens techniques de tiers, une externalisation de la fonction compliance n'est pas admissible.

Section 6.2.6. Le contrôle des risques

Sous-section 6.2.6.1. Système de gestion des risques

158. Les établissements mettent en place un système 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 gestion de garder sous maîtrise l'ensemble des risques auxquels l'établissement est ou pourrait être exposé. Ce système de gestion des risques doit permettre à l'établissement de recenser, analyser et traiter les principaux risques identifiés au regard des objectifs de l'établissement.

159. Le système 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 en ce compris notamment les succursales, filiales, agents, distributeurs et bureaux de représentation.

160. Afin de permettre à l'organe de gestion de garder sous strict contrôle certains aspects clés des risques sectoriels de l'établissement, le système de gestion des risques doit couvrir de manière spécifique pour l'établissement les risques liés à l'adéquation des fonds propres, la liquidité de l'établissement, la gestion des flux de paiement et de monnaie électronique de l'établissement ainsi que le bon fonctionnement du dispositif de protection des fonds des utilisateurs de services de paiement.

161. Lorsque les établissements octroient des crédits liés aux services de paiement dans les conditions définies aux articles 10, paragraphe 3 et 24-6, paragraphe 1, de la LSP, le système de gestion des risques implique également la mise en œuvre d'un solide dispositif permettant :
    - de gérer, détecter et rapporter aux organes de gestion et de surveillance tout dépassement de l'activité de crédit en référence à l'appétit aux risques défini et aux limites internes définies et approuvées par ces organes (cf. paragraphes 13 et 40 de la présente circulaire) ;

- de gérer et supporter sur une base continue les risques liés à cette activité de crédit en vue de garantir une adéquation permanente tant en temps normal qu'en temps de crise des fonds propres et des liquidités conformément aux exigences internes et légales ;
- de détecter et gérer les activités de crédit dont les échéances contractuelles et légales sont dépassées ;
- de fournir aux organes de gestion, de surveillance et à l'autorité compétente à tout instant le montant de cette activité de crédit, des crédits dont les échéances sont dépassées, des fonds propres et liquidités internes permettant de répondre aux exigences légales et de couvrir les risques liés à cette activité de crédit.

Lorsque les établissements octroient des crédits liés aux services de paiement dans les conditions définies aux articles 10, paragraphe 3 et 24-6, paragraphe 1, de la LSP, cette activité est supportée par des politiques d'acceptation de risques qui définissent quels risques peuvent être pris et les critères et conditions qui s'appliquent en la matière ainsi que par des politiques qui définissent les mesures à prendre lorsqu'un utilisateur de service de paiement ne respecte pas ou signale à l'établissement qu'il n'est plus en mesure de rembourser son crédit/de respecter son engagement comprenant une procédure de régularisation des défauts de remboursement, de suivi de la régularisation de ceux-ci ainsi que d'escalade. En complément, les établissements disposent d'un dispositif pour la gestion et le provisionnement des défauts de remboursement susmentionnés.

Sous-section 6.2.6.2. Fonction indépendante de contrôle des risques

162. En fonction de l'organisation de l'établissement, la CSSF pourra demander à certains établissements, en référence au principe de proportionnalité (cf. paragraphe 3 de la présente circulaire), de doter leur établissement d'une fonction indépendante et permanente de contrôle des risques.

Sous-section 6.2.6.3. Gestion des risques de la fonction informatique

163. Les établissements mettent en place un système de gestion des risques liés aux TIC et à la sécurité en ligne avec les exigences du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier et des circulaires de la CSSF relatives aux exigences en matière de gestion des risques liés aux TIC et à la sécurité.

Section 6.2.7. La fonction d'audit interne

Sous-section 6.2.7.1. La charte d'audit interne

164. 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 en dernier ressort par l'organe de surveillance.

165. La charte d'audit interne doit au minimum :

- définir la position de la fonction d'audit interne dans l'organigramme de l'établissement tout en en précisant les caractéristiques clés (indépendance, objectivité, intégrité, compétence, autorité, suffisance des ressources) ;
- conférer à la fonction d'audit interne le droit d'initiative et l'autoriser à examiner toutes les activités et fonctions de l'établissement, y compris celles de ses succursales, bureaux de représentation et agents ou distributeurs au Luxembourg et à l'étranger ainsi que les activités et fonctions faisant l'objet d'une externalisation, à accéder à tous les documents, pièces, procès-verbaux des organes consultatifs et décisionnels de l'établissement, à voir toutes les personnes travaillant pour l'établissement, dans la mesure requise pour l'exercice de sa mission ;
- définir les lignes de communication hiérarchiques et fonctionnelles des conclusions qui se dégagent des missions d'audit ;
- définir les relations avec les fonctions compliance et de contrôle des risques ;
- définir les conditions et circonstances applicables lorsqu'il est fait recours à des experts externes ou prestataires de services ;
- définir la nature des travaux et les conditions dans lesquelles la fonction d'audit interne peut fournir de la consultance interne ou effectuer d'autres missions spéciales ;
- définir les responsabilités et lignes de reporting du « Chief Internal Auditor » ;
- établir le droit pour le « Chief Internal Auditor » de contacter directement et de sa propre initiative le président de l'organe de surveillance ou, le cas échéant, les membres des comités spécialisés ainsi que la CSSF ;
- préciser les standards professionnels reconnus qui gouvernent le fonctionnement et les travaux de l'audit interne ;
- préciser les procédures à respecter en matière de coordination et de coopération avec le réviseur d'entreprises agréé.

166. 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 au Luxembourg et à l'étranger.

167. La charte d'audit interne doit être mise à jour dans les meilleurs délais pour tenir compte des changements survenus. Toutes les modifications doivent être approuvées par l'organe de surveillance en dernier ressort. Elles sont portées à la connaissance de tous les membres du personnel.

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

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

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

- le suivi du respect des lois et réglementations ainsi que des exigences prudentielles imposées par la CSSF ;
- l'efficacité et l'efficience du dispositif en matière d'administration centrale, de gouvernance et de contrôle interne, en ce compris la fonction de contrôle des risques et la fonction compliance ;
- la sauvegarde des valeurs et des biens ainsi que la protection des fonds des utilisateurs de services de paiement et le respect des réserves de liquidités internes ;
- l'adéquation des fonds propres ;
- l'enregistrement correct et exhaustif des opérations et la production d'informations financières et prudentielles correctes, complètes, pertinentes, compréhensibles et disponibles sans délai à l'organe de surveillance et aux comités spécialisés, le cas échéant, à l'organe de gestion et à la CSSF ;
- le respect des politiques et procédures.

170. Lorsqu'il existe au sein 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 la fonction 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.

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

171. L'ensemble des missions d'audit interne est planifié et exécuté selon un plan d'audit interne. Le plan est établi par le responsable de la fonction d'audit interne pour une période pluriannuelle (en principe trois ans) avec comme objectif de couvrir l'ensemble des activités et des fonctions, en tenant compte à la fois des risques que présentent une activité ou une fonction et de l'efficacité de l'organisation et du contrôle interne en vigueur pour cette activité ou fonction (approche basée sur le risque). Le plan tient compte des avis de l'organe de surveillance ou du comité spécialisé, le cas échéant, ainsi que de l'organe de gestion. Le plan couvre toutes les matières présentant un intérêt prudentiel (y compris les observations et les demandes de la CSSF) et tient compte également des développements et innovations prévus ainsi que des risques qui peuvent en découler. Le champ d'intervention de la fonction d'audit interne ne peut être limité dans son étendue.

172. De par sa criticité, la thématique de la protection des fonds détenus par l'établissement pour le compte des utilisateurs de services de paiement ou par le biais d'un autre prestataire de services de paiement pour l'exécution d'opérations des paiements doit faire l'objet d'une revue appropriée annuelle de la part de l'audit interne. La revue de la thématique susmentionnée inclut notamment la revue des accès (aux comptes bancaires y afférents, aux systèmes critiques), les procédures de réconciliations mises en place, les éventuels contrôles clés automatisés/intégrés au système ou application informatique, le respect à tout moment des articles 14 et/ou 24-10 de la LSP et l'adéquation des procédures manuelles et automatisées de suivi des niveaux de protection qui soient adaptées en fonction de la méthode de protection des fonds utilisée.

173. Le plan d'audit interne est discuté avec l'organe de gestion et, le cas échéant, le comité spécialisé et approuvé en dernier ressort par l'organe de surveillance. Il est à revoir sur une base annuelle et à adapter en fonction des développements et des urgences. Toute adaptation, y inclus toute mission reportée ou annulée, est à revoir par l'organe de gestion et le comité spécialisé, le cas échéant, avant d'être approuvée par l'organe de surveillance. L'approbation implique que l'organe de gestion 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 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 l'organe de surveillance : missions annulées, missions reportées ainsi que missions dont le champ d'application a été changé de manière significative.

174. Le plan d'audit interne 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 la fonction d'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.

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

    Dans le cas de figure où le plan d'audit interne de l'établissement luxembourgeois est établi de manière coordonnée avec celui de sa maison mère ou du groupe auquel il appartient, l'organe de surveillance conserve la pleine responsabilité du respect des exigences réglementaires ainsi que des principes énoncés dans cette circulaire.

176. La fonction d'audit interne informe l'organe de gestion et, le cas échéant, le comité spécialisé de façon régulière sur l'exécution du plan d'audit interne.

177. 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.

178. Chaque mission doit faire l'objet d'un rapport écrit de la fonction d'audit interne destiné, en règle générale, aux personnes contrôlées, à l'organe de gestion ainsi que - éventuellement sous forme de synthèse - à l'organe de surveillance (et au comité spécialisé, le cas échéant). Ces rapports sont à rédiger en français, allemand ou anglais et sont également à tenir à disposition du réviseur d'entreprises agréé et de la CSSF.

    Ce rapport écrit comprend non seulement une description des insuffisances et anomalies constatées, mais également des recommandations et des propositions sur les mesures correctrices à prendre incluant un échéancier de mise en place de ces mesures, de même qu'en règle générale une prise de position des personnes contrôlées. Le rapport donne également une indication de l'importance relative des anomalies et déficiences constatées ainsi que des recommandations et des mesures correctrices.

179. 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 qui sera remis à l'organe de gestion et à l'organe de surveillance. Une copie de ce rapport est remise à la CSSF, et cela, en accord avec la circulaire CSSF 15/614 et tenue à disposition du réviseur d'entreprises agréé.

Sous-section 6.2.7.3. Organisation de la fonction d'audit interne

180. 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 au sein de la présente circulaire.

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

182. En cas d'externalisation des tâches opérationnelles de la fonction d'audit interne, les établissements doivent se référer à la circulaire CSSF 22/806, les prestataires de services réalisent leurs travaux dans le cadre du plan d'audit interne de l'établissement, en suivant un programme de travail, en documentant leurs travaux de façon détaillée et en rédigeant des rapports pour chaque mission. Ces rapports sont à rédiger en français, allemand ou anglais et sont à remettre à l'organe de gestion, au comité spécialisé, le cas échéant, et à l'organe de surveillance. Lorsque ces prestataires externes exercent la profession de réviseur d'entreprises agréé, ils doivent à tous égards être indépendants du réviseur d'entreprises et du cabinet de révision agréés de l'établissement.

Chapitre 7. Exigences spécifiques

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

183. La structure organisationnelle, en termes de succursales, de réseau d'agents, de distributeurs et de bureaux de représentation, est appropriée et justifiée par rapport aux stratégies et principes directeurs. Elle est claire et transparente aux yeux de l'ensemble des parties prenantes. La structure juridique, organisationnelle et opérationnelle doit permettre et promouvoir une gestion efficace, saine et prudente des activités. Elle ne doit pas entraver la bonne gouvernance de l'établissement, en particulier la capacité de l'organe de gestion à gérer et à contrôler efficacement les activités (et les risques) de l'établissement.

184. Les principes directeurs que l'organe de surveillance arrête en matière de structure organisationnelle (en termes de succursales et de réseau d'agents, de distributeurs et de bureaux de représentation) 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 sont garanties ;
- tout flux d'information de gestion matérielle est documenté et peut être fourni promptement à l'organe de surveillance, à l'organe de gestion, aux fonctions de contrôle interne ou à toute autorité compétente, à leur demande.

185. Les principes directeurs que 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 sont soumises à une analyse approfondie et un suivi continu des risques, en particulier ceux liés à la criminalité financière. Qu'il s'agisse d'activités pour compte propre ou pour compte d'utilisateurs des services de paiement, l'établissement doit comprendre l'utilité de ces structures et maitriser les risques accompagnant leur création et leur fonctionnement opérationnel.

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

Sous-chapitre 7.2. Gestion des conflits d'intérêts

Section 7.2.1. Exigences générales

186. La politique en matière de gestion des conflits d'intérêts couvre l'ensemble des conflits d'intérêts, pour des raisons économiques, personnelles, professionnelles ou politiques, qu'ils soient persistants ou liés à un événement unique. Une attention particulière doit être portée aux conflits d'intérêts entre l'établissement et ses parties liées et ses prestataires de services. Cette politique est applicable à tout le personnel ainsi qu'aux membres de l'organe de gestion et aux membres de l'organe de surveillance.

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

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

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

190. La politique traitant les conflits d'intérêts détermine également les procédures de déclaration et d'escalade applicable au sein de l'établissement. Lorsqu'ils sont ou ont été confrontés à un conflit d'intérêts, les membres du personnel en informent leur supérieur hiérarchique promptement et de leur propre initiative. Les membres de l'organe de gestion et de l'organe de surveillance qui sont sujets à un conflit d'intérêts en informent respectivement l'organe de gestion et 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.

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

Section 7.2.2. Exigences spécifiques relatives aux conflits d'intérêts en relation avec des parties liées

192. Les transactions avec des parties liées sont soumises pour approbation 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.

193. Tout changement matériel relatif à des transactions significatives effectuées avec des parties liées doit être porté à l'attention de l'organe de surveillance dans les meilleurs délais.

194. Les transactions avec des parties liées doivent être réalisées de façon objective 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 répondent à au moins un des critères suivants :

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

- ont pour effet de porter atteinte à la solvabilité, à la situation des liquidités ou aux capacités de gestion des risques de l'établissement sur le plan réglementaire ou interne ;
- dépassent les capacités de gestion et de contrôle des risques ou sortent des domaines d'activités habituels de l'établissement ;
- sont contraires aux principes d'une gestion saine et prudente dans l'intérêt de l'établissement.

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

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

196. 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 le cas échéant les limites correspondantes.

197. La procédure d'approbation des nouveaux produits définit en particulier les modifications d'activités sujettes à la procédure d'approbation, les aspects à prendre en considération, les principales questions à examiner ainsi que le déroulement de la procédure d'approbation, y compris les responsabilités de toutes les parties concernées. Les principales questions à examiner incluent notamment la conformité avec la réglementation, la protection des fonds des utilisateurs de service de paiement, 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, ainsi que la disponibilité d'outils internes adéquats et de connaissances techniques suffisantes pour comprendre et contrôler les risques afférents.

198. 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/cartographie des risques en la matière. De même, l'organe de gestion et le cas échéant la fonction de contrôle des risques procèdent 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.

199. Aucune nouvelle activité ne doit être entreprise avant que l'approbation n'ait été donnée par l'organe de gestion, après avoir entendu toutes les parties concernées et en particulier les fonctions de contrôle interne, et que les moyens mentionnés au paragraphe précédent soient disponibles.

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

Chapitre 8. Les exigences en matière de protection des fonds

Sous-chapitre 8.1. Exigences générales

201. Conformément aux exigences des articles 14 et 24-10 de la LSP et en ligne avec les principes directeurs en matière de protection de fonds approuvés par l'organe de surveillance, l'établissement est tenu de mettre en place des mécanismes assurant à tout moment la protection de l'ensemble des fonds reçus de la part des utilisateurs de services de paiement ou par le biais d'un autre prestataire de services de paiement pour l'exécution d'opérations de paiement et/ou en échange de la monnaie électronique émise.

    Ceci implique que l'établissement doit être en permanence en mesure d'identifier clairement et précisément l'ensemble des fonds des utilisateurs de services de paiement. L'établissement doit veiller à porter une attention particulière aux aspects de continuité des dispositions de protection des fonds et à assurer une capacité de réaction appropriée en cas de révocation des contrats par les contreparties utilisées dans le cadre des mécanismes de protection des fonds.

202. Les établissements instituent des mécanismes de contrôle interne adéquats et efficients et un cadre de suivi général qui fournit des informations appropriées à l'organe de gestion et à l'organe de surveillance. Ces mécanismes de contrôle interne incluent notamment des processus de contrôle des opérations exécutées ainsi que des processus de réconciliation des fonds reçus de la part des utilisateurs de services de paiement ou par le biais d'un autre prestataire de services de paiement pour l'exécution d'opérations de paiement et de monnaie électronique avec les informations issues des contreparties auprès desquels les fonds sont protégés (c.-à-d. établissement de crédit, entreprise d'assurance, etc.). Ces processus font l'objet de procédures claires déterminant les responsables de ces processus, les différentes parties intervenantes, les procédures formelles d'escalade et de validation liées à ces processus.

    Sans préjudice de la section 4.2.3. de la présente circulaire, l'établissement nomme au sein de son organe de gestion un membre responsable du suivi et de l'encadrement des processus de contrôle interne permettant d'assurer le respect des exigences de protection des fonds.

    Ces mécanismes de contrôle interne doivent permettre d'identifier à tout moment et sans délai les fonds qui ne sont pas protégés au travers d'une des manières prévues aux articles 14 et 24-10 de la LSP. Ils sont déployés en considérant l'organisation de l'établissement, la nature, l'échelle, le volume et la complexité des activités et des risques de l'établissement.

203. Eu égard au volume et/ou à la complexité des services de paiement ou de monnaie électronique prestées par l'établissement, les mécanismes de contrôle interne mentionnés au paragraphe 202 de la présente circulaire doivent reposer sur la mise en place de contrôles et de réconciliations quotidiennes.

    La mise en place de réconciliations hebdomadaires peut le cas échéant être envisagée sur la base d'une analyse justifiée et documentée des risques validée par l'organe de gestion et l'organe de surveillance. Les organes de gestion et de surveillance veillent à assurer l'allocation de ressources appropriées et suffisantes à ces contrôles et réconciliations qui sont sujets à une revue et/ou validation suivant le principe de 4 yeux.

Il est par ailleurs recommandé aux établissements de se doter d'outils informatisés de contrôle et de réconciliation. Le recours à des processus de contrôle manuel est à considérer à titre exceptionnel.

204. Sans préjudice des exigences définies à la section 5.3.1. de la présente circulaire, l'accès aux écritures comptables, comme aux systèmes extra-comptables ainsi que les pouvoirs de signature permettant de mouvementer les fonds des utilisateurs de service de paiement est strictement limité selon les principes du « need-to-know and least privilege » et systématiquement soumis au principe des 4 yeux, sous la responsabilité formelle d'au moins un membre de l'organe de gestion.

205. En référence au principe de proportionnalité repris au paragraphe 3 de la présente circulaire, il pourra être demandé à certains établissements de mettre en place un dispositif de gestion des risques de contrepartie dans le cadre de l'ouverture de compte de ségrégation auprès d'établissements de crédit et/ou en référence au recours à des contreparties dans le cadre de l'établissement de mécanismes d'assurance et/ou de garantie comparable.

Une analyse (due diligence) et un suivi régulier de la qualité du ou des établissements de crédit, assureurs ou autres contreparties utilisés par l'établissement dans le cadre de la protection des fonds sont considérés comme une bonne pratique de gestion saine et prudente.

Sous-chapitre 8.2. Protection des fonds par le recours à des comptes dits « de ségrégation » (cf. articles 14, paragraphe 1, lettre a) et 24-10, paragraphe 1, lettre a), de la LSP)

206. Les comptes de ségrégation sont ouverts au nom de l'établissement pour le seul bénéfice des utilisateurs de services de paiement. Les contrats en référence à ces comptes établissent clairement le nom et l'adresse de l'établissement de crédit auprès duquel les comptes de ségrégation sont ouverts, la nature de ces comptes et la propriété des fonds qui y sont déposés.

Lorsque l'établissement investit ces fonds en actifs à faible risque, liquides et sûrs, de telles dispositions s'appliquent mutatis mutandis de sorte que les actifs sont déposés sur un dépôt distinct ouvert au nom de l'établissement pour le seul bénéfice des utilisateurs de services de paiement.

207. L'établissement veille à ce qu'aucune des clauses contractuelles, que ce soit dans les conditions générales ou particulières, ne puissent remettre en question les exigences telles que définies aux articles 14 et 24-10 de la LSP. À ce titre, et dans le cas où l'établissement de crédit ne fournit pas un contrat spécifique de « ségrégation », l'établissement doit veiller à obtenir toutes les confirmations écrites et signées nécessaires et suffisamment explicites de la part de ce dernier afin de s'assurer de la conformité du niveau de protection des fonds déposés avec la LSP.

L'établissement doit évaluer et pouvoir démontrer la conformité de l'ensemble de ses comptes de ségrégation et des contrats y afférent à la LSP.

208. L'accès aux fonds et/ou actifs placés dans le cadre de la protection des fonds est limité aux seules personnes dont la fonction le requiert et est limité au strict nécessaire afin de leur permettre d'accomplir les tâches qui leur incombent. Ces accès sont rigoureusement encadrés, formalisés et régulièrement revus par l'établissement et communiqués à l'organe de gestion.

Il est attendu que toute opération manuelle et/ou significative permettant de mouvementer les fonds et/ou actifs placés dans le cadre de la protection des fonds ne puisse être exécutée que suivant un principe de 4 yeux et sous la stricte validation a priori d'au moins un membre de l'organe de gestion.

209. Dans le cas de recours à des agents, distributeurs ou succursales, l'établissement assume l'entière responsabilité de la protection des fonds et doit s'assurer en permanence des procédures appliquées par ces agents ou distributeurs et en particulier que les fonds soient correctement protégés et dans les délais impartis.

210. Conformément aux exigences des articles 14 et 24-10 de la LSP, les fonds reçus ne doivent à aucun moment être mélangés avec les fonds de personnes autres que les utilisateurs de services de paiement pour le compte desquels les fonds sont détenus.

Cette exigence s'applique notamment aux fonds détenus en lien avec d'autres activités, ainsi qu'aux frais et commissions applicables et liés aux services de paiement et de monnaie électronique. En conséquence, il appartient à l'établissement de déployer des processus organisationnels et opérationnels appropriés permettant de respecter ces exigences.

Ces processus sont à revoir et adapter dans le cadre du déploiement de nouveaux produits en référence aux exigences du sous-chapitre 7.3 de la présente circulaire.

211. Il est recommandé aux établissements de revoir les conflits d'intérêts potentiels provenant d'une politique interne, de l'établissement ou de son groupe, de concentration systématique des comptes de ségrégation auprès de mêmes établissements de crédit ainsi que dans le cadre d'investissements des fonds dans des actifs à faible risque et sûrs émis ou distribués par un même groupe financier.

212. Aux fins des présentes exigences en matière de protection, sont notamment à considérer par les établissements lorsqu'ils ont pris la décision de protéger les fonds en les investissant dans des actifs à faible risque, liquides et sûrs, les actifs répondant au minimum aux critères suivants :

- des titres de créance émis ou garantis par les administrations centrales, les banques centrales, les organisations internationales, les banques multilatérales de développement ou les autorités régionales ou locales des États membres ;
- les parts d'OPCVM investissant exclusivement dans ces titres de créances

sous réserve que l'évaluation du risque de crédit soit continue, que le rating de ces actifs soit élevé et que les fonds investis ne soient pas soumis à un risque de marché indu.

213. L'établissement qui entend protéger les fonds des utilisateurs de services de paiement et les investir dans des actifs à faible risque, liquides et sûrs établit les critères minimaux de qualité auxquels les actifs doivent répondre en référence au paragraphe 212 en conformité avec les principes directeurs en matière de protection des fonds approuvés par l'organe de surveillance en référence au paragraphe 13 de la présente circulaire.

L'établissement met également en place une politique de gestion des risques liés au placement des fonds dans ces actifs à faible risque, liquides et sûrs et assure un suivi adéquat de la volatilité des prix de ces actifs afin de garantir à tout moment la protection des fonds des utilisateurs de services de paiement et d'assurer la liquidité nécessaire à l'exécution des services de paiement et de monnaie électronique.

214. Il est recommandé aux établissements de détenir les fonds des utilisateurs de services de paiement en dépôts en compte de ségrégation et/ou investis en actifs à faible risque et sûr dans la devise des fonds des utilisateurs de services paiement afin de minimiser l'exposition des actifs ségrégués au risque de change. Dans le cas contraire, l'établissement devra mettre en place des mécanismes de protections complémentaires contre le risque de change afin de limiter l'exposition à ce risque pour les actifs ségrégués.

Sous-chapitre 8.3. Protection des fonds par le recours à une assurance ou un autre type de garantie (cf. article 14, paragraphe 1, lettre b) et 24-10, paragraphe 1, lettre b), de la LSP)

215. Le montant de la garantie fournie par l'assurance ou la garantie comparable doit être revu régulièrement en considérant, le cas échéant, les délais de négociation contractuelle. L'organe de gestion de l'établissement doit en effet s'assurer que le montant de couverture est à tout moment suffisant pour protéger l'ensemble des fonds détenus pour le compte des utilisateurs de services de paiement ou par le biais d'un autre prestataire de services de paiement.

216. Une attention particulière doit être portée aux définitions des bénéficiaires de l'assurance ou de la garantie, aux évènements susceptibles de déclencher le versement des indemnités de la part de l'entreprise d'assurance ou de l'entreprise offrant la garantie comparable aux délais relatifs à ces versements, à l'existence d'un compte auprès d'un établissement de crédit dédié au versement des indemnités en cas d'exécution de l'assurance ou de la garantie. Il est ainsi rappelé que le produit de la garantie/assurance doit être payable sur un compte dédié et séparé ouvert auprès d'un établissement de crédit au nom de l'établissement pour le bénéfice des utilisateurs de services de paiement. Ce compte, sous le strict contrôle de l'établissement, doit être clairement défini et documenté au sein de la documentation liée à la présente assurance ou garantie comparable.

217. L'ensemble des dispositions contractuelles et toute condition applicable au contrat de garantie ou d'assurance doit faire l'objet d'un examen par un expert juridique. Cet examen sera pris en compte par l'organe de gestion qui doit assurer que toute clause restrictive ou en nullité pouvant diminuer le montant de la protection ou de la garantie sera éliminée.

    L'établissement doit évaluer, documenter et pouvoir démontrer la conformité de l'ensemble de ses dispositions contractuelles à la LSP.

Chapitre 9. Reporting légal

218. En complément des dispositions de la circulaire CSSF 15/614 « Documents à fournir à la CSSF après la clôture de l'exercice financier », les rapports et attestation suivants sont communiqués annuellement en référence à la présente circulaire à la CSSF :

    (a) L'évaluation annuelle des risques liés aux TIC et à la sécurité conformément à l'article 105-1, paragraphe 2, de la LSP et aux exigences de la circulaire CSSF 25/880 « Relationship management of payment service users and PSP ICT assessment ».

(b) L'attestation annuelle de conformité avec les exigences de la présente circulaire émise et signée par l'ensemble des membres de l'organe de gestion en référence au paragraphe 71 de la présente circulaire.

Cette attestation est à soumettre à la CSSF dans les meilleurs délais et au plus tard le dernier jour du troisième mois qui suit la date de clôture de l'exercice financier de l'établissement.

(c) Les rapports de synthèse des fonctions de compliance et d'audit interne établis conformément au paragraphe 129 de la présente circulaire et respectivement signés par le « Chief Compliance Officer » et le « Chief Internal Auditor ». Ces informations sont à soumettre à la CSSF dans les meilleurs délais et au plus tard le dernier jour du troisième mois qui suit la date de clôture de l'exercice financier de l'établissement. Les informations en question sont à établir en français, allemand ou anglais.

Partie III. Entrée en vigueur

219. La présente circulaire est applicable à partir du 30 juin 2026.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général