COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Luxembourg, le 18 juillet 2012

A tous les PSF de support

CIRCULAIRE CSSF 12/544

Concerne : Optimisation par une approche par les risques de la surveillance exercée sur les « PSF de support »

Mesdames, Messieurs,

Cette circulaire s'adresse à tous les PSF exerçant une ou plusieurs activités de PSF de support, telles que définies dans les articles 29-1, 29-2, 29-3 ou 29-4 de la loi du 5 avril 1993 relative au secteur financier **et** codifiés de type « I » par la CSSF (se référer aux numéros signalétiques tels que publiés sur le site www.cssf.lu).

La CSSF a pour mission de protéger la stabilité financière des entreprises surveillées et du secteur financier dans son ensemble ainsi que de veiller au respect de la réglementation financière applicable aux entreprises surveillées.

Les PSF de support offrent des services davantage de nature opérationnelle et technique que financière et ne sont pas, par nature, des professionnels du secteur financier. Leurs services s'adressent à tout type d'entreprises appartenant ou non au secteur financier. C'est la prestation de certains services à des clients professionnels du secteur financier qui les qualifie alors eux-mêmes de professionnels du secteur financier et les fait ainsi entrer dans le périmètre de surveillance de la CSSF.

Or, cette prestation de services peut accentuer ou engendrer un certain nombre de risques pour le secteur financier. Le degré de risque que chaque PSF de support fait courir au secteur financier peut varier fortement d'un PSF de support à un autre, selon notamment la nature des services prestés ainsi que la part de marché et l'organisation du PSF de support concerné. Dans un souci de clarté, précisons qu'il ne s'agit pas des risques des clients professionnels financiers du PSF de support - tel que la dépendance au fournisseur, la perte d'expertise, etc... qui doivent être adressés par les clients professionnels financiers eux-mêmes – mais, bien des risques du PSF de support pouvant avoir un impact direct ou indirect sur les clients professionnels financiers et qui représentent donc un risque pour ces derniers.

Forte de ces constats, la CSSF relevait dès avril 2008[1] « qu'il devenait prioritaire pour la CSSF comme pour les PSF de support de recentrer la surveillance prudentielle par rapport aux enjeux et risques encourus par le secteur financier uniquement et qu'une réflexion était engagée en ce sens au sein de la CSSF ». Elle recommandait ainsi aux PSF de support « de se préparer à disposer d'un processus d'évaluation et de gestion des risques pour les activités prestées au secteur financier ».

La concrétisation de la réflexion engagée à ce sujet au sein de la CSSF se traduit par la volonté d'optimiser le cadre de la surveillance exercée sur les PSF de support en introduisant un nouveau concept d'approche par les risques (« risk-based approach »). Cette démarche s'inscrit dans le contexte du nombre croissant des PSF de support depuis la création des statuts y relatifs ainsi que de la diversité des activités prestées par ceux-ci.

Ce recentrage de la surveillance par rapport aux enjeux et risques engendrés pour le secteur financier[2] s'appuie sur :

1. l'application du principe de proportionnalité selon l'importance de l'activité fournie par le PSF de support au secteur financier : l'importance de l'activité peut être qualifiée d'une part du point de vue du secteur financier (importance des activités sous-traitées au PSF de support pour les clients) et d'autre part du point de vue du PSF de support (poids du secteur financier dans la clientèle totale du PSF de support) ;

2. la prise en compte de l'auto-évaluation et de la gestion par le PSF de support des risques qu'il fait courir au secteur financier, celles-ci devant faire annuellement l'objet d'un **rapport d'analyse de risques (RAR)** par le PSF de support ; une description des activités prestées auprès du secteur financier, de l'organisation et de l'infrastructure du PSF de support – à fournir annuellement dans un **rapport descriptif (RD)** – facilitera la compréhension et l'analyse des risques reportés dans le RAR. En application du principe de proportionnalité, la CSSF s'attend à ce que le volume du RD soit proportionnel à l'importance de l'activité fournie par le PSF de support au secteur financier ;

3. la définition des règles pratiques concernant la mission des réviseurs d'entreprises agréés auprès de ces entités, et l'établissement d'un **compte rendu analytique de révision (CRA)**. Le CRA a pour objectif de rendre compte des constatations essentielles du réviseur d'entreprises agréé, permettant un jugement précis et fondé sur l'organisation, le système de contrôle interne, la situation financière et

1. Circulaire CSSF 08/350 relative à des précisions concernant les modifications apportées par la loi du 13 juillet 2007 relative aux marchés d'instruments financiers au statut des PSF visés par les articles 29-1, 29-2, 29-3 ou 29-4 de la loi du 5 avril 1993 relative au secteur financier (ci-après « la LSF») et dénommés « PSF de support » ; Modification des modalités de surveillance prudentielle des PSF de support.
2. Les termes « professionnels financiers » ou « secteur financier » sont à considérer au sens de cette circulaire comme incluant les clients entreprises d'assurances et de réassurances, à moins d'une mention expresse en sens contraire. Sont visés les risques engendrés pour les professionnels financiers de droit luxembourgeois et de droit étranger clients du PSF de support.

les risques du PSF de support contrôlé, qui peuvent avoir un impact direct ou indirect sur ses clients professionnels du secteur financier. En application du principe de proportionnalité, la CSSF s'attend à ce que le volume du CRA soit proportionnel à l'importance de l'activité fournie par le PSF de support au secteur financier.

Ce recentrage de la surveillance comprend deux étapes.

La présente circulaire (étape 1) spécifie, d'une part, le contenu du rapport d'analyse de risques et, d'autre part, le contenu du rapport descriptif, sachant que ces deux documents constituent une source importante d'informations tant pour la direction du PSF de support dans le cadre de sa fonction de gestion que pour la CSSF dans l'exercice de sa mission de surveillance prudentielle.
Dans ses dispositions finales et transitoires, la circulaire prévoit la remise à la CSSF des premiers rapports d'analyse de risques et des premiers rapports descriptifs dès 2013.

Une seconde circulaire (étape 2) viendra définir les règles pratiques concernant la mission des réviseurs d'entreprises agréés auprès des PSF de support et le contenu du compte rendu analytique de révision, complétant ainsi le dispositif d'optimisation de la surveillance.

SOMMAIRE

I. Principes généraux

Le PSF de support produit annuellement :

- un rapport sur son système de gestion des risques et sur l'auto-évaluation de ses risques au secteur financier (ci-après « rapport d'analyse de risques » ou « RAR ») ;

- un rapport décrivant son organisation administrative et comptable, son système de contrôle interne, son infrastructure informatique (à usage interne ou supportant les services aux clients), ses activités et sa situation financière (ci-après « rapport descriptif» ou « RD »).

Le PSF de support est engagé sur la véracité de tous les éléments inclus dans ces deux rapports. A ce titre, la direction[3] y apposera sa signature.

Le RAR et le RD sont émis à l'usage des organes de direction et d'administration/gérance du PSF de support concerné ainsi que de la CSSF. Les minutes du Conseil d'administration (ou de gérance) devront mentionner la transmission du RAR aux membres du conseil.

D'une manière générale, le PSF de support est le rédacteur principal du RAR et du RD. Il pourra cependant, s'il le souhaite, s'adjoindre le soutien d'un externe pour lui confier la rédaction de certaines parties descriptives, sans aucunement déroger à sa responsabilité en ce qui concerne la véracité de tous les éléments y inclus.

Les PSF de support auront un délai maximal de trois mois à partir de la date de clôture comptable[4] pour envoyer le RAR et le RD à la CSSF.

Dès qu'il en a connaissance, le PSF de support informera la CSSF de tout retard annoncé en indiquant les raisons et la durée probable du retard.

Le RAR et le RD doivent être transmis à la CSSF sur support papier **et** par voie de transmission électronique. Les modalités de transmission électronique feront l'objet d'une circulaire dédiée.

3. Le terme « direction » signifie dans cette circulaire "les personnes chargées de la gestion journalière et agréées en vertu de l'article 19(2) de la LSF".
4. Se référer aux dispositions finales et transitoires en ce qui concerne le délai applicable pour la première année.

II. Rapport d'analyse de risques au secteur financier (« RAR »)

Le PSF de support[5] fournit dans son rapport d'analyse de risques :

- une description de son système de gestion des risques ;
- son auto-évaluation des risques qu'il peut faire courir à ses clients du secteur financier.

II.A. Système de gestion des risques au secteur financier

Le PSF de support fournit une description de son système de gestion des risques au secteur financier qui porte au minimum sur les éléments suivants :

- les rôles et responsabilités des différentes parties prenantes (acteurs) à ce système ;
- les méthodes et procédures en place pour l'identification, l'évaluation, la validation, la limitation, le suivi et la communication des risques ;
- les outils de gestion et de documentation des risques éventuellement utilisés.

Concernant les rôles et responsabilités, le PSF de support indique notamment :

- Le membre de la direction responsable de la gestion des risques ;
- Si la charge de la gestion des risques est confiée à une ou des personne(s) en interne. Ces personnes doivent jouir, d'un point de vue hiérarchique, de l'indépendance nécessaire pour pouvoir assumer leur responsabilité de façon adéquate ;
- Si la charge de la gestion des risques est confiée à un externe expert en matière de gestion des risques qui est alors à nommer.

Il est en effet permis que des établissements de taille réduite qui exercent une activité à faible risque, renoncent à confier la fonction de gestion des risques à un service ou à un employé travaillant à temps plein. Ces établissements peuvent recourir à des externes experts en matière de gestion des risques, sous réserve qu'une telle externalisation ait été autorisée par la CSSF au préalable.

L'externalisation de la gestion des risques ne doit pas remettre en cause le principe du caractère continu du processus de gestion des risques, en se limitant par exemple à un seul exercice d'évaluation des risques par an.

La gestion des risques ne peut en aucun cas être confiée au réviseur d'entreprises agréé ou à l'audit interne du PSF de support ou de son groupe. A la demande du PSF de support, son réviseur d'entreprises agréé pourra donc prendre uniquement en charge la description du système de gestion des risques ; il ne pourra pas prendre en charge ou apporter son soutien à la gestion des risques (incluant l'identification, l'évaluation, la validation, la limitation, le suivi et la communication des risques).

5. Chaque fois que le terme « PSF de support » est mentionné dans les dispositions des parties II.A et II.B ci-après, il y a lieu de comprendre « PSF de support, y compris ses succursales ».

II.B. Auto-évaluation des risques directs et indirects au secteur financier

Le PSF de support doit fournir une description et une auto-évaluation des risques qu'il peut faire courir à ses clients du secteur financier, qu'il s'agisse de risques directs ou indirects, tels que définis respectivement aux points II.B.1 et II.B.2.

Il devra estimer l'importance, ou autrement dit la criticité, de chaque risque identifié et devra pour cela considérer les deux variables suivantes :

- la probabilité de survenance du risque (P), et ;
- l'impact du risque (I) s'il venait à se réaliser, sachant que ce dernier peut être de plusieurs types : impact financier, légal et réglementaire, opérationnel, etc.

Le PSF de support devra déterminer le niveau de probabilité et le(s) niveau(x) d'impact(s) applicables sur des échelles de probabilité et d'impacts fournies en **annexe 1**. L'importance d'un risque sera ensuite déterminée en multipliant le niveau de probabilité retenu par le niveau d'impact retenu (P x I). Si plusieurs types d'impact sont applicables pour un seul et même risque, le PSF de support retiendra le plus élevé pour le calcul de l'importance du risque.

Ainsi par exemple, si un risque a une probabilité de survenance de 4, un impact financier de 3 et un impact légal de 5, l'importance du risque sera de 4 (probabilité) multiplié par 5 (impact légal car le plus élevé), soit une importance égale à 20.

Pour chaque risque identifié, le PSF de support calculera :

- l'importance brute du risque, c'est-à-dire sans prise en compte des contrôles existants (risque brut) ;
- l'importance nette du risque, c'est-à-dire avec prise en compte des moyens existants pour réduire ou transférer le risque (risque net) ; si aucun moyen n'existe au moment de l'évaluation, l'importance nette est égale à l'importance brute ;
- si applicable, l'importance attendue du risque, c'est-à-dire en anticipant les effets d'un plan d'actions proposé pour diminuer ou transférer le risque, lorsque l'importance nette du risque a été considérée comme trop élevée donc inacceptable.

Les risques à inclure dans le rapport d'analyse de risques[6] seront limités à 20 risques pour les risques directs (tels que définis au point 1.1. ci-après) et à 5 risques pour les risques indirects (tels que définis au point 1.2. ci-après). Les risques à reporter sont alors ceux ayant obtenu les scores les plus élevés lors du calcul de l'importance nette (résultats les plus élevés des opérations (P_{nette} x $I_{net\ le\ plus\ élevé}$)).

Toutefois, tout risque direct ou indirect dont l'impact net est égal ou supérieur à 6 tout en ayant simultanément une probabilité nette égale ou supérieure à 5 est également à

6. Se référer aux dispositions finales et transitoires en ce qui concerne les risques à inclure dans le premier rapport d'analyse de risques.

rapporter, même si les limites de 20 et de 5 risques mentionnées au paragraphe précédent sont par ailleurs atteintes.

Un risque rapporté dans le RAR pourrait ne plus l'être l'année suivante si les mesures de mitigation mises en place dans l'intervalle le classent hors des risques à rapporter selon les critères évoqués ci-dessus ou encore si le risque n'est plus pertinent du fait d'un changement d'activités ou d'organisation. Toute suppression d'un risque d'un RAR à l'autre devra faire l'objet d'une explication motivant une telle suppression.

Pour chacun des risques à inclure dans le rapport d'analyse de risques, les informations suivantes sont à rapporter dans une fiche de risque (un exemple se trouve en annexe **2**) :

- un numéro de risque (identifiant) :
- le titre du risque ;
- une description brève mais claire du risque ;
- une indication si ce risque concerne tous les clients professionnels du secteur financier du PSF de support ou seulement quelques-uns d'entre eux, qui sont alors à citer nommément ;
- la catégorie du risque, à choisir parmi les catégories présentées aux points 1.1 et 1.2. ;
- le niveau de probabilité, le(s) niveau(x) d'impact et l'importance du risque (P x I) définis par le PSF sans prise en compte des contrôles existants (risque brut), et une justification de cette importance (l'importance pour les clients professionnels du secteur financier tel que le PSF l'estime est à considérer ici et non pas l'importance pour le PSF de support) ;
- les moyens existants mis en œuvre par le PSF pour réduire (mitigation) ou transférer (assurance) et suivre ces risques ;
- la référence aux travaux d'audit interne effectués pour vérifier l'existence et l'efficacité de ces aspects de mitigation ;
- le niveau de probabilité, le(s) niveau(x) d'impact et l'importance du risque (P x I) définis par le PSF suite à la prise en compte des moyens existants pour réduire ou transférer le risque (risque net) ; si aucun moyen n'existe au moment de l'évaluation, le risque net est égal au risque brut ;
- la stratégie argumentée de réponse au risque compte tenu de son importance nette : accepter le risque (car il est de faible importance ou en dehors du contrôle du PSF), mettre en place un plan d'actions pour réduire (mitigation) ou transférer le risque (assurance), éviter le risque (en abandonnant une activité par exemple) ;
- une description brève mais claire du plan d'actions futures visant à diminuer ou transférer le risque, lorsqu'il n'est pas jugé acceptable ;
- l'importance (P x I) attendue du risque une fois le plan d'actions réalisé.

Les fiches de risques seront fournies dans l'ordre des identifiants des risques.

Un registre des risques (un exemple se trouve en **annexe 3**) présentera un récapitulatif des risques par ordre d'importance nette décroissante.

Tout événement survenant durant l'année et modifiant significativement le profil de risques au secteur financier du PSF (par exemple, apparition d'un nouveau risque significatif ou réévaluation à la hausse de l'importance d'un risque déjà identifié) doit être communiqué à la CSSF par le PSF de support, sans attendre l'émission du prochain rapport d'analyse de risques. La communication comprendra une description du ou des risque(s) nouveau(x) ou réévalué(s) sous la forme d'une fiche de risque, telle que présentée ci-avant.

1. Risques directs

Les risques directs sont les risques portant directement sur les activités prestées auprès du secteur financier et qui ont donc un impact direct sur les clients bénéficiaires de ces activités.

L'analyse de risques doit porter sur les catégories de risques suivantes :

- **D1 (« direct 1 »)-Risques stratégiques / politique commerciale :** exemple : le marché principal du PSF n'est pas le secteur financier, celui-ci n'étant alors pas prioritaire en termes de moyens mis en œuvre pour délivrer des services de qualité.

- **D2-Risques opérationnels – Ressources Humaines :** est concerné le personnel directement nécessaire à la prestation des services au secteur financier. Exemples : sous-effectif, personnel non qualifié, utilisation excessive d'intérimaires, absence de remplaçant pour une fonction clé, etc.
- **D3-Risques opérationnels – Processus :** sont concernés les processus directement liés à la prestation des services au secteur financier. Exemples : absence de documentation des procédures clés, insuffisance du contrôle interne, etc.

- **D4-Risques opérationnels – Continuité des opérations :** sont concernées les opérations nécessaires à la délivrance des services au secteur financier. Exemples : Business Continuity Plan inexistant / incomplet / non testé ; Disaster Recovery Plan inexistant / incomplet / non testé ; absence de coordination avec le BCP/DRP du client, éventuellement du groupe ou d'un sous-contractant, etc.

- **D5-Risques opérationnels – Sous-traitance en cascade :** est concernée la sous-traitance à une société tierce (hors ou intra groupe) d'opérations nécessaires à la délivrance des services au secteur financier. Exemples : maîtrise insuffisante de la sous-traitance en cascade (contrôle insuffisant par le PSF de la qualité des services rendus ; respect du secret professionnel ; contrat de service entre le PSF et son sous-traitant), etc.

- **D6-Risques opérationnels – Systèmes d'informations :** sont concernés les systèmes d'informations à usage externe décrits au point 3.3. de la section III.B. Les risques relatifs aux domaines suivants sont à considérer :

- **D6.1-Sécurité des informations** (confidentialité, intégrité, continuité, traçabilité) : exemples : absence/inadéquation de la politique de sécurité, de gestion et de suivi ; de la ségrégation physique et logique des environnements clients en cas de mutualisation ; de la sécurité physique ; de la sécurité logique des systèmes et communications entrantes et sortantes, de la gestion des incidents de sécurité, etc. ;

- **D6.2-Acquisition, développement et maintenance des systèmes** (adéquation des solutions aux besoins du client) : exemples : absence/inadéquation des procédures d'acquisition ou de développement de nouvelles applications, de modification d'applications déjà existantes, de contrôle de qualité et de mise en exploitation, de documentation, etc. ;

- **D6.3-Procédures d'exploitation** (gestion des traitements batchs, des sauvegardes, des impressions de rapports, etc.) : exemples : absence/inadéquation des procédures de planification, séquencement et contrôle ; procédures de contrôle des sorties et des traitements, procédures de sauvegarde, de restauration et d'archivage ; procédures de gestion d'incidents, etc. ;

- **D6.4-Support technique du système d'informations :** exemples : absence/inadéquation des procédures de maintenance des logiciels de base ; maintenance et administration des bases de données ; typologie du réseau interne ; maintenance et surveillance du réseau de communication ; assistance utilisateur et péri-informatique, etc.

- **D7-Autres catégories de risques pertinentes** au regard des activités fournies par le PSF de support à ses clients du secteur financier.

2. Risques indirects

Les risques indirects sont les risques relatifs à l'organisation et à l'administration du PSF de support ou à ses prestations hors secteur financier **et** dont l'impact engendre un risque indirect pour ses clients professionnels du secteur financier.

L'analyse de risques doit porter sur les catégories de risques suivantes :

- **I1 (« Indirect 1 »)-Risques stratégiques et de gouvernance :** exemples : risque de défaillance/désengagement du PSF suite à une décision de gestion, une stratégie de développement, de rachat ou de restructuration inadaptée (prise localement ou au niveau groupe si applicable), absence de (ou inefficacité de) son propre système de gestion des risques, etc.

- **I2-Risques financiers :** exemples : risque de défaillance/désengagement dû à une mauvaise situation financière (rentabilité), des investissements risqués, etc.

- **I3-Risques légaux et réglementaires :** exemples : risque de défaillance/désengagement dû à des poursuites/sanctions ou à la perte de l'agrément de PSF de support, etc.

- **I4-Risques opérationnels – Ressources Humaines :** est concerné le personnel nécessaire à l'organisation et à l'administration du PSF de support. Exemples : troubles organisationnels majeurs dus à un problème de sous-effectif, personnel non qualifié, absence de remplaçant pour une fonction clé, etc.

- **I5-Risques opérationnels – Processus :** sont concernés les processus liés à l'organisation et à l'administration du PSF de support. Exemples : troubles organisationnels majeurs dus à l'absence de documentation des procédures clés, l'insuffisance du contrôle interne, etc.

- **I6-Risques opérationnels – Continuité des opérations :** sont concernées les opérations nécessaires à une bonne organisation et administration du PSF de support. Exemples : Business Continuity Plan inexistant / incomplet / non testé ; Disaster Recovery Plan inexistant / incomplet / non testé ; si applicable, absence de coordination avec le BCP/DRP du groupe ou d'un sous-contractant (non redondance de la ligne de communication vers le système comptable outsourcé, pas de locaux/matériels de remplacement), etc.

- **I7-Risques opérationnels – Sous-traitance en cascade** : est concernée la sous-traitance à une société tierce (hors ou intra groupe) d'opérations nécessaires à une bonne organisation et administration du PSF de support. Exemples : maîtrise insuffisante de la sous-traitance en cascade (contrôle insuffisant par le PSF de la qualité des services rendus ; confidentialité des informations ; contrat de service entre le PSF et son sous-traitant ; etc.).

- **I8-Risques opérationnels – Systèmes d'informations :** sont concernés les systèmes d'informations à usage interne décrits au point 2.8 de la section III.B. Les risques relatifs aux domaines suivants sont à considérer :

  - **I8.1-Sécurité des informations** (confidentialité, intégrité, continuité, traçabilité) : exemples : absence/inadéquation de la politique de sécurité, de gestion et de suivi ; de la sécurité physique ; de la sécurité logique des systèmes et communications entrantes et sortantes ; de la gestion des incidents de sécurité, etc. ;

  - **I8.2-Acquisition, développement et maintenance des systèmes** (adéquation des solutions aux besoins du PSF) : exemples : absence/inadéquation des procédures d'acquisition ou de développement de nouvelles applications, de modification d'applications déjà existantes, de contrôle de qualité et de mise en exploitation, de documentation, etc. ;

- **I8.3-Procédures d'exploitation** (gestion des traitements batchs, des sauvegardes, des impressions de rapports, etc.) : exemples : absence/inadéquation des procédures de planification, séquencement et contrôle ; procédures de contrôle des sorties et des traitements, procédures de sauvegarde, de restauration et d'archivage ; procédures de gestion d'incidents, etc. ;

- **I8.4-Support technique du système d'information :** exemples : absence/inadéquation des procédures de maintenance des logiciels de base ; maintenance et administration des bases de données ; typologie du réseau interne ; maintenance et surveillance du réseau de communication ; assistance utilisateur et péri-informatique, etc. ;

- **I9-Risques liés à une prestation hors secteur financier :** exemples : risque financier (pénalités sur un contrat important,…), risque indirect de réputation (« reputational spillover »), en cas d'échec médiatisé d'un projet majeur hors secteur financier, etc.

- **I10-Autres catégories de risques pertinentes** au regard de l'organisation et de l'administration du PSF de support ou de son groupe et dont l'impact pour le PSF de support engendre un risque indirect pour ses clients professionnels du secteur financier.

La CSSF se réserve le droit d'évaluer et de commenter la qualité du système de gestion des risques du PSF de support et le caractère suffisant ou non des mesures de mitigation des risques mises en place par le PSF de support.

III. Rapport descriptif (« RD »)

III.A. Schéma du rapport descriptif

Le rapport descriptif doit être établi suivant le schéma ci-après. Le schéma en question correspond aux informations minimales qui doivent être détaillées par le PSF de support dans son rapport. Il peut être adapté à la nature et à la complexité des activités ainsi qu'à la structure de l'entreprise. Le cas échéant, le PSF de support doit compléter le schéma indiqué par les points qu'il jugera nécessaires. Lorsqu'un point déterminé du schéma ne s'applique pas au PSF de support, celui-ci le mentionne explicitement.

1. Evénements significatifs

2. Organisation et administration
   2.1. Description de l'actionnariat
   2.2. Direction en charge de la gestion journalière
   2.3. Organigramme du PSF de support et du groupe auquel il appartient
   2.4. Administration centrale
   2.5. Organisation administrative

2.6. Fonction comptable
2.7. Contrôle interne
2.8. Système informatique à usage interne

3. Activités prestées auprès du secteur financier
3.1 Description des activités prestées
3.2 Partenariats / sous-traitance en cascade
3.3 Système informatique à usage externe
3.4 Plan de continuité et de recouvrement (BCP/DRP)

4. Rapports périodiques à communiquer

5. Analyse des comptes annuels

6. Obligations professionnelles en matière de prévention du blanchiment de capitaux et du financement du terrorisme

7. Obligations professionnelles en matière de règles de conduite

8. Relations avec les entreprises liées

9. Succursales à l'étranger

10. Filiales à l'étranger

III.B. Commentaires relatifs au rapport descriptif

1. Evénements significatifs

Le PSF de support indique le cas échéant les événements significatifs qui ont eu lieu au cours de l'exercice sous revue et susceptibles d'impacter sa situation. Il s'agit par exemple de décisions stratégiques, de réorganisations importantes, du lancement ou de l'arrêt d'une activité, d'opérations de fusion/acquisition ou de collaboration/partenariat.

Les évènements significatifs pouvant faire apparaître des risques pour les clients professionnels financiers du PSF de support doivent être repris dans le rapport d'analyse de risques du PSF de support tel que demandé au chapitre II de la présente circulaire (c'est-à-dire qu'ils sont pris en compte dans le système de gestion des risques tel que décrit au point II.B.1 et détaillés dans l'auto-évaluation des risques telle que décrite au point II.B.2).

Lorsqu'il n'y a pas eu d'événements significatifs au cours de l'exercice sous revue, le PSF de support mentionnera ce fait expressément.

2. Organisation et administration

Le PSF de support fournira sous ce point une vue d'ensemble de sa structure opérationnelle, décisionnelle et de gouvernance (hors système de gestion des risques couvert dans le rapport d'analyse de risques).

2.1. Description de l'actionnariat

Le PSF de support fournit une description de son actionnariat direct ainsi que du groupe auquel il appartient ; cette structure sera présentée sous forme d'un organigramme avec liens capitalistiques.

Un exemplaire du rapport sur les comptes annuels, des comptes annuels et du rapport de gestion de l'actionnaire majoritaire direct sont à annexer au rapport descriptif.

Dans le cas où son actionnaire majoritaire direct n'est pas soumis à l'obligation d'établir un rapport de gestion, le PSF de support fournira cependant - avec le rapport sur les comptes annuels et les comptes annuels de son actionnaire majoritaire direct - des informations sur l'évolution des affaires et la situation de l'actionnaire et des indications concernant cet actionnaire sur :

- les événements importants survenus après la clôture de l'exercice ;
- l'évolution prévisible de la société ;
- les activités en matière de recherche et de développement ;
- en ce qui concerne les acquisitions d'actions propres, les indications visées à l'article 49-5 paragraphe (2) de la loi modifiée du 10 août 1915 concernant les sociétés commerciales ;
- l'existence des succursales de la société.

2.2. Direction en charge de la gestion journalière

Le PSF de support fournit une description des attributions de la direction en charge de la gestion journalière et le périmètre des pouvoirs nécessaires au bon accomplissement de sa mission que le conseil d'administration (ou conseil de gérance) lui aura délégué.

Il précise notamment s'il y a lieu :

- les limites éventuelles imposées par le conseil d'administration (ou conseil de gérance) aux décisions locales du PSF de support dans le contexte d'un groupe ;
- les décisions du conseil d'administration (ou conseil de gérance) imposées localement au PSF de support et qui peuvent aller à l'encontre de la réglementation luxembourgeoise.

Si ces limites et/ou décisions sont de nature à créer un risque direct ou indirect pour les activités prestées auprès du secteur financier par le PSF de support, ce dernier doit les reprendre dans son rapport d'analyse de risques tel que demandé au chapitre II de la présente circulaire (c'est-à-dire qu'ils sont pris en compte dans le système de gestion des

risques tel que décrit au point II.B.1 et détaillés dans l'auto-évaluation des risques telle que décrite au point II.B.2).

2.3. Organigramme du PSF de support et du groupe auquel il appartient

Le PSF de support fournit sous forme graphique :

- son organigramme interne, en indiquant les lignes hiérarchiques et fonctionnelles ainsi que les effectifs par service ;
- l'organigramme de son groupe montrant son positionnement au sein du groupe.

2.4. Administration centrale

Le PSF de support fournit une brève description de l'organisation de son administration centrale.

2.5. Organisation administrative

Le PSF de support fournit une brève description de son organisation administrative.

En cas de recours à un outsourcing de services administratifs, le PSF de support doit également en faire une brève description et précise :

- si cet outsourcing fait l'objet d'un contrat (SLA) ;
- la surveillance mise en place au niveau du PSF pour encadrer les services qui font l'objet d'un outsourcing ;
- si la sous-traitance est clairement mentionnée dans les conditions générales des contrats clients du secteur financier, dans le cas où cet outsourcing aurait pour conséquence la localisation à l'étranger de données concernant des clients professionnels du secteur financier[7], ou l'accès depuis l'étranger à ces données.

2.6. Fonction comptable

Le PSF de support doit donner une brève description du fonctionnement de sa fonction comptable.

En cas de recours à un outsourcing de la fonction comptable, le PSF de support doit également en faire une brève description et précise :

- s'il est en mesure d'avoir un accès permanent aux pièces comptables et aux états financiers ;
- si cet outsourcing fait l'objet d'un contrat (SLA) ;
- la surveillance mise en place au niveau du PSF pour encadrer les services qui font l'objet d'un outsourcing ;
- si la sous-traitance est clairement mentionnée dans les conditions générales des contrats clients du secteur financier, dans le cas où cet outsourcing aurait pour conséquence la localisation à l'étranger de données concernant des clients professionnels du secteur financier[7], ou l'accès depuis l'étranger à ces données.

7. Par exemple le nom du client.

2.7. Contrôle interne

Le PSF de support fournit une description de la manière dont son système de contrôle interne est organisé.

2.7.1 Procédures internes

Le PSF de support indique sous ce point l'existence d'un manuel de procédures couvrant l'ensemble des activités opérées au sein de la société et qui peuvent avoir un impact direct ou indirect sur les clients professionnels du secteur financier.

Le PSF de support mentionne également si, conformément à ses obligations :

- il a bien mis en place un programme de formation de ses employés notamment au respect de la confidentialité des données des clients professionnels du secteur financier et à la prévention du blanchiment et du financement du terrorisme ;
- les contrats employés incluent bien une clause de confidentialité ainsi qu'une mention des poursuites pénales encourues en cas de violation du secret professionnel[8].

2.7.2 Systèmes internes d'informations et de contrôle de gestion

Le PSF de support fournit une description des systèmes internes d'informations et de contrôle de gestion, en particulier une description du *management information system* (MIS).

2.7.3 Comité d'audit

Dans l'hypothèse où le PSF de support dispose d'un comité d'audit[9] qui lui est propre (un éventuel comité d'audit au niveau groupe n'est pas concerné ici), il décrit la composition, les modalités de fonctionnement, la fréquence et l'ordre du jour des réunions de ce comité.

2.7.4 Audit interne

Le PSF de support fournit une description de la fonction d'audit interne (in-house, soutien de la maison-mère, recours à un expert externe ou recours à des tiers professionnels auquel cas il y a lieu de décrire la coordination avec le responsable du suivi des travaux).

8. Tel qu'en dispose l'article 41(1) de la LSF.
9. Conformément au point 6 de la circulaire IML 98/143 et à l'article 74 de la loi du 18 décembre 2009 relative à la profession de l'audit.

2.7.5 Rapports

Le PSF de support insérera en annexe du rapport descriptif les deux rapports suivants[10] :

- le rapport écrit de la direction sur l'état du contrôle interne ;
- une copie du rapport de synthèse sur les contrôles effectués par l'audit interne au cours de l'exercice écoulé[11]. Le rapport de synthèse devra être présenté sous forme d'un tableau synthétisant les principales recommandations. Le rapport sera divisé en deux parties : la première partie aura pour objet le suivi des recommandations émises lors des interventions de l'audit interne pour l'année en cours, la deuxième partie aura quant à elle pour vocation le suivi des recommandations émises lors des interventions d'audit interne effectuées au cours des années antérieures. Comme mentionné préalablement, chacune de ces deux parties devra être présentée sous forme d'un tableau. Les colonnes du tableau devront au moins mentionner dans cet ordre :
  - la date de la mission ;
  - le périmètre ou le domaine de la mission ;
  - la référence (le numéro) de l'observation ;
  - l'observation ;
  - le niveau de risque (par exemple : « élevé, moyen ou faible ») ;
  - les recommandations ;
  - les commentaires de la direction du PSF de support ;
  - le délai d'implémentation ;
  - si applicable, la référence du risque lié identifié par ailleurs dans le rapport d'analyse de risques du PSF de support.

Le PSF de support devra également insérer en annexe les documents suivants :

- une copie de la ou des lettre(s) de mission confiée(s) à l'auditeur interne ;
- le plan pluriannuel d'audit interne entériné par la direction et/ou le conseil d'administration (ou conseil de gérance) ; le plan d'audit doit notamment impérativement couvrir les aspects de diminution (mitigation) des principaux risques identifiés dans le rapport d'analyse de risques du PSF de support ;
- la charte d'audit interne.

Le PSF de support annexera également un tableau concernant les personnes désignées comme responsables de certaines fonctions en vertu des circulaires de la CSSF[12].

Le PSF de support devra enfin annexer une liste à jour des membres de la direction en charge de la gestion journalière.

10. Conformément au point 8 de la circulaire IML 98/143.
11.Conformément aux points 5.4.7.d) et 5.4.9 de la circulaire IML 98/143.
12. Pour ce faire, le PSF pourra se baser sur le tableau B 4.6 tel que défini dans la circulaire CSSF 09/424.

2.8. Systèmes informatiques à usage interne

Le PSF de support donne une description des systèmes et traitements informatiques à usage interne.

Sont à considérer comme systèmes informatiques à usage interne les systèmes qui supportent l'organisation et l'administration du PSF de support. Ils ne font donc pas partie de l'infrastructure informatique qui supportent, partiellement ou exclusivement, les activités prestées auprès des clients du PSF de support.

A titre d'exemple, et sans que cette liste soit limitative, les systèmes suivants sont considérés comme des systèmes informatiques à usage interne : les systèmes de comptabilité, de gestion du personnel et de paiement du PSF de support ; les systèmes de gestion des commandes clients, de gestion des achats, de gestion de la relation client mais aussi les serveurs de messagerie, serveurs de fichiers internes, site internet du PSF de support (hors utilisation pour des services prestés à ses clients), postes de travail du personnel.

2.8.1 Tableau de synthèse

Le PSF de support fournit un tableau de synthèse des systèmes informatiques à usage interne (voir un exemple en **annexe 4**) mettant en relation les fonctions principales nécessaires au fonctionnement interne du PSF de support, avec les éléments informatiques qui les opèrent. Ces éléments informatiques se décomposent en éléments d'infrastructure physique ou virtuelle (les plates-formes informatiques et leur système d'exploitation) et en éléments logiciels (les applications informatiques ou chaînes de programmes).

2.8.1.1. Infrastructure physique

Les éléments matériels (ordinateurs et périphériques) physiques principaux qui opèrent une ou plusieurs fonctions principales seront identifiés par leur marque, leur modèle, leur système d'exploitation (y compris numéro de version), leur mode de redondance (aucune, hot/cold standby, cluster,…) et la raison de la redondance (criticité des fonctions, répartition de la charge, mixte).

Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.

Les postes de travail ne doivent pas être repris dans le descriptif s'ils n'opèrent pas au moins une fonction principale à l'activité.

2.8.1.2. Infrastructure virtuelle

a) Les éléments matériels physiques principaux qui supportent des machines virtuelles opérant une ou plusieurs fonctions principales seront identifiés par les mêmes informations que celles mentionnées au 1er paragraphe du point 2.8.1.1 ci-dessus.

   Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.

   Il précise également le nombre de machines virtuelles hébergées par chaque machine physique.

   Les postes de travail ne doivent pas être repris dans le descriptif s'ils n'opèrent pas au moins une fonction principale à l'activité.

b) Les éléments matériels virtuels principaux qui opèrent une ou plusieurs fonctions principales feront l'objet d'une description simplifiée qui précisera au moins le type de machine virtuelle (VM, XEN, etc.) et leur système d'exploitation (y compris numéro de version).

   Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.
   Il précise également le numéro ou nom d'identification de la machine physique qui héberge les machines virtuelles.

2.8.1.3. Les éléments logiciels

Concernant les éléments logiciels qui opèrent une ou plusieurs fonctions principales, le tableau de synthèse fournira les informations relatives :

- au nom du logiciel ou progiciel ;
- au développement :
  - développement (avec ou sans recours à des sous-traitants) ;
  - progiciel (avec indication du nom du fournisseur) ;
  - progiciel modifié (si plus de 20% des fonctionnalités ont été modifiées), avec indication des intervenants dans les modifications (interne, fournisseur, mixte).
- aux modifications importantes opérées depuis l'exercice précédent.

2.8.1.4. Outsourcing et localisation des systèmes

Le recours à un outsourcing[13] des systèmes ou traitements informatiques internes ainsi que la localisation des systèmes doivent être précisés pour chaque système concerné. Le tableau de synthèse fournira notamment pour chaque élément matériel (physique ou virtuel) et logiciel une réponse aux questions suivantes :

- L'élément est-il dédié au PSF de support ou partagé avec d'autres entités ?
- Le PSF recourt-il à un outsourcing et si oui, quelle en est la nature (hébergement seulement ou prestation d'opérations) ?
- Qui opère l'élément : le PSF ou un tiers prestataire de services à préciser (une entité du groupe est à considérer comme un tiers prestataire de services) ?
- Où est localisé le système ? Indiquer les locaux (du PSF, d'un tiers prestataire y compris d'une entité du groupe ?) et le pays si le système est à l'étranger.
- En cas d'outsourcing, existe-t-il un plan de reprise (transfert à un autre fournisseur ou reprise en gestion propre), dans l'hypothèse où la continuité ou la qualité de la prestation de service du prestataire risquerait d'être compromise ?

2.8.2 Architecture réseau et connexions externes

Le PSF de support fournit une description et/ou un schéma de l'architecture réseau du PSF de support comportant les éléments principaux de sécurité (DMZ, firewalls, IDS, routers, proxy, etc.). Au cas où il ne serait pas possible ou utile de différencier l'architecture réseau nécessaire au fonctionnement interne du PSF de celle nécessaire aux activités prestées auprès du secteur financier, il peut être renvoyé au point 3.3.3.

Le PSF de support liste les connexions utiles au fonctionnement interne vers ou depuis l'extérieur (y compris avec son groupe le cas échéant), en précisant le contrôle qu'il exerce sur ces accès (Active Directory séparé, ouverture/fermeture des lignes de communication, logs, etc.) et les mesures de redondance de ces connexions.

3. Activités prestées auprès du secteur financier

3.1. Description des activités prestées

Le PSF de support fournit une description précise du type et du volume de ses activités. Il faudra d'une part faire la distinction entre les activités prestées auprès du secteur financier, du secteur des assurances et les autres activités et d'autre part distinguer entre les activités qui requièrent un agrément en tant que PSF de support et celles qui ne le requièrent pas.

13. Au sens de la circulaire CSSF 05/178.

Le PSF de support précise également le cas échéant le mode de prestation des services. A titre d'exemple :

- pour un agent administratif : services de type « Business Process Outsourcing » délivrés sur le site du PSF de support et sur son propre système informatique mutualisé ;
- pour un opérateur de systèmes informatiques primaires : mise à disposition et gestion d'une « Infrastructure as a Service » localisée dans ses locaux en mode dédié ou partagé ;
- pour un opérateur de systèmes informatiques secondaires : gestion du réseau sur le site du client ;
- pour un agent de communication à la clientèle : impression et mise sous pli de courriers à destination des clients du client professionnel financier, sur ses propres systèmes et dans ses propres locaux.

Lorsqu'il y a eu un changement de la nature des activités, l'abandon d'une activité ou le lancement d'activités nouvelles ou encore lorsqu'il y a eu des événements exceptionnels ou significatifs au cours de l'exercice sous revue, il en sera rapporté au point 1. « Evénements significatifs ».

Le PSF de support fournit également une liste nominative de ses clients des secteurs financiers luxembourgeois ou étrangers pour lesquels il preste des services nécessitant un agrément PSF, précisant en outre pour chacun d'eux :

- le secteur d'activité concerné (financier/assurances) ;
- le pays de résidence (Luxembourg/étranger) ;
- la nature de la prestation (activités principales prestées) ;
- la localisation de la prestation ;
- et si elle est offerte via une communication à distance ou sur site.

Pour chaque type d'agrément de PSF de support dont il dispose, le PSF de support annexe la copie d'un contrat client portant sur des prestations de service nécessitant un tel agrément.

3.2. Partenariats / sous-traitance en cascade

Le PSF de support indiquera l'existence éventuelle de partenariat ou de sous-traitance en cascade (avec des sociétés externes ou au sein du groupe) pour la prestation des activités au secteur financier et en précisera la nature (expertise, mise à disposition de profils, prestation requérant l'agrément).

Il précisera également :

a. ses propres effectifs (en nombre d'ETP) nécessaires directement à la prestation des services aux clients (tous secteurs confondus),
b. le pourcentage des effectifs définis au point a. alloué à la prestation de services au secteur financier (effectif dédié),
c. le pourcentage des effectifs définis au point a. alloué à la fois à la prestation de services au secteur financier **et** à la prestation de services à d'autres secteurs (effectif commun),

d. les effectifs (en nombre d'ETP) de sous-contractants éventuels utilisés sur une base permanente par le PSF de support dans la prestation de services au secteur financier,
e. le pourcentage de l'effectif mis à disposition du secteur financier (effectif défini au point b.) que les sous-contractants représentent,
f. le pourcentage de l'effectif commun mis à disposition du secteur financier et des autres secteurs (effectif défini au point c.) que les sous-contractants représentent.

Enfin, le PSF de support décrit les éléments lui permettant de maîtriser cette sous-traitance en cascade, tels que :

- le contrôle par le PSF de la qualité des services prestés par le sous-traitant (notamment vérification de l'existence d'indicateurs de mesure de la performance) ;
- la prise en compte par le sous-traitant des risques pour le client (existence d'une analyse de risques et transmission des résultats au PSF de support) ;
- le respect du secret professionnel, notamment si le sous-traitant ou partenaire n'a pas lui-même le statut de PSF de support ;
- l'existence d'un contrat de service entre le PSF et son sous-traitant ;
- l'information des clients sur l'existence de cette sous-traitance en cascade ;
- le maintien d'une substance PSF suffisante au sein du PSF de support.

3.3. Systèmes informatiques à usage externe

Le PSF de support donne une description des systèmes et traitements informatiques à usage externe.

Sont à considérer comme systèmes informatiques à usage externe :

1. les systèmes qui supportent partiellement ou exclusivement les activités prestées pour les clients professionnels du secteur financier du PSF de support, indépendamment de leur appartenance au client ou au PSF ou de leur localisation,
2. et pour lesquels le PSF de support a la responsabilité du bon fonctionnement vis-à-vis du client.

Ces deux conditions sont cumulatives pour déterminer si un système est qualifié de système à usage externe au sens de cette circulaire et est alors concerné par cette section.

Le terme « système » peut ici se limiter à un logiciel si la prestation porte uniquement sur un logiciel.

A titre d'exemple, un agent administratif qui offre des services de comptabilité de fonds à des professionnels du secteur financier sur son propre système comptable en ses locaux – système qu'il utilisait déjà auparavant et qu'il continue à utiliser pour sa propre activité – pourrait de prime abord considérer ce système comptable comme un système interne. Cependant, ce système est bien à considérer comme un système externe au sens de cette circulaire, puisqu'il supporte aussi une activité prestée auprès du secteur financier, que l'agent administratif est responsable de son bon fonctionnement et qu'il a le pouvoir de décider du système supportant la prestation.

De même, un agent administratif qui offre des services de comptabilité de fonds à des professionnels du secteur financier sur son propre système comptable, mais qui sous-traite lui-même la gestion de son système à un tiers, doit considérer ce système comme concerné par cette section. En effet, indépendamment du recours à cette sous-traitance, l'agent administratif garde la responsabilité du fonctionnement du système vis-à-vis de ses clients et conserve éventuellement un pouvoir de décision quant au choix du système supportant la prestation.

3.3.1 Tableau de synthèse

Le PSF de support fournit un tableau de synthèse (voir l'exemple en **annexe 5**) mettant en relation les fonctions principales (y compris techniques comme des firewalls, par exemple) nécessaires aux prestations qu'il offre au secteur financier, avec les éléments informatiques qui les opèrent. Ces éléments informatiques se décomposent en éléments d'infrastructure physique ou virtuelle (les plates-formes informatiques et leur système d'exploitation) et en éléments logiciels (les applications informatiques ou chaînes de programmes).

3.3.1.1. Infrastructure physique

Les éléments matériels (ordinateurs et périphériques) principaux qui opèrent une ou plusieurs fonctions principales seront identifiés par leur marque, leur modèle, leur système d'exploitation (y compris numéro de version), leur mode de redondance (aucune, hot/cold standby, cluster, …) et la raison de la redondance (criticité des fonctions, répartition de la charge, mixte).

Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.

Le nombre total de clients et le nombre de clients du secteur financier supportés par chaque élément sera précisé.

Les postes de travail ne doivent pas être repris dans le descriptif s'ils n'opèrent pas au moins une fonction principale à l'activité.

3.3.1.2. Infrastructure virtuelle

a) Les éléments matériels physiques principaux qui supportent des machines virtuelles opérant une ou plusieurs fonctions principales seront identifiés par les mêmes informations que celles mentionnées au 1er paragraphe du point 3.3.1.1 ci-dessus.

Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.

Il précise également pour chaque machine physique le nombre de machines virtuelles hébergées, le nombre total de clients et le nombre de clients du secteur financier supportés ou toute information pertinente pour l'évaluation du risque de concentration des clients sur une même machine (par exemple le volume de transactions traitées sur cette machine).

Les postes de travail ne doivent pas être repris dans le descriptif s'ils n'opèrent pas au moins une fonction principale à l'activité.

b) Les éléments matériels virtuels principaux qui opèrent une ou plusieurs fonctions principales feront l'objet d'une description simplifiée qui précisera au moins le type de machine virtuelle (VM, XEN, etc.) et leur système d'exploitation (y compris numéro de version).

Lorsque les informations fournies sont les mêmes pour plusieurs éléments, le tableau de synthèse les présente une seule fois en indiquant alors le numéro ou nom d'identification et le nombre total des éléments concernés.

Il précise également le numéro ou nom d'identification de la machine physique qui héberge les machines virtuelles.

Il précise enfin le nombre total de clients et le nombre de clients du secteur financier supportés par chaque machine virtuelle ou toute information pertinente pour l'évaluation du risque de concentration des clients sur une même machine (par exemple le volume de transactions traitées sur cette machine).

3.3.1.3. Les éléments logiciels

Les éléments logiciels qui opèrent une ou plusieurs fonctions principales feront l'objet d'une description simplifiée qui reprendra, lorsqu'elles sont disponibles, les informations relatives :

- à la gestion des données : type de gestion (base de données, fichiers indexés, fichiers séquentiels, combinaison de différents types) et nom du produit ;
- au type d'environnement, au langage de programmation ;
- au mode de traitement : temps réel, différé (batch) ou mixte avec, pour le dernier cas, indication des fonctions qui sont traitées en batch ;
- à l'architecture : client-serveur et nombre de niveaux, en indiquant, par niveau, les fonctions servies (par exemple client-serveur à trois niveaux : présentation, application, données) et l'identification du matériel supportant chaque fonction ;

- au développement :
  - développement (avec ou sans recours à des sous-traitants) ;
  - progiciel (avec indication du nom du fournisseur) ;
  - progiciel modifié (si plus de 20% des fonctionnalités ont été modifiées), avec indication des intervenants dans les modifications (interne, fournisseur, mixte).
- aux modifications importantes opérées depuis l'exercice précédent.

3.3.1.4. Outsourcing et localisation des systèmes

Le recours à un outsourcing[14] des systèmes ou traitements informatiques externes ainsi que la localisation des systèmes doivent être précisés pour chaque système concerné. Le tableau de synthèse fournira notamment pour chaque élément matériel (physique ou virtuel) et logiciel une réponse aux questions suivantes :

- L'élément est-il dédié au PSF de support (et par extension à ses clients dans le cadre de ses prestations) ou partagé avec d'autres entités ?
- Le PSF recourt-il à un outsourcing et si oui, quelle en est la nature (hébergement seulement ou prestation d'opérations) ?
- Qui opère l'élément : le PSF ou un tiers prestataire de services à préciser (une entité du groupe est à considérer comme un tiers prestataire de services) ?
- Où est localisé le système ? Indiquer les locaux (du PSF, d'un tiers prestataire y compris d'une entité du groupe ?) et le pays si le système est à l'étranger.
- En cas d'outsourcing, existe-t-il un plan de reprise (transfert à un autre fournisseur ou reprise en gestion propre), dans l'hypothèse où la continuité ou la qualité de la prestation de service du prestataire risquerait d'être compromise ?

3.3.2 Schéma fonctionnel des flux

Les principaux liens (interfaces) qui existent entre les fonctions et, par conséquent, les systèmes renseignés conformément au point 3.3.1 seront décrits par le PSF de support dans un schéma fonctionnel des flux.

Lorsque toutes les fonctions sont intégrées au sein d'un logiciel unique fonctionnant sur un seul matériel (p. ex. : cas d'un progiciel bancaire), il n'est pas nécessaire de détailler les flux internes, mais uniquement les flux entrants et sortants du système.

3.3.3 Architecture réseau et connexions externes

Le PSF de support fournit une description et/ou un schéma de son architecture réseau comportant les éléments principaux de sécurité (DMZ, firewalls, IDS, routers, etc.).

14. Au sens de la circulaire CSSF 05/178.

Il liste les connexions utiles au fonctionnement des activités prestées auprès du secteur financier vers ou depuis l'extérieur (y compris avec son groupe le cas échéant), en précisant le contrôle qu'il exerce sur ces accès. Il fournit notamment une description brève des mécanismes de sécurité mis en place, tant au niveau physique (firewall, routeurs,…), qu'au niveau logique (détecteurs d'intrusions, anti-virus, authentification des clients, confidentialité des communications, intégrité et non-répudiation des transactions,…) et organisationnel (suivi des journaux/log, configuration des équipements de sécurité, génération des clés ou certificats d'authentification des clients, monitoring des systèmes,…).

3.4. Plan de continuité et de recouvrement (BCP/DRP)

Le PSF de support fournit une description du plan de continuité qu'il a établi en cas de sinistre de ses propres locaux, respectivement en cas d'impossibilité d'accéder à ses propres locaux (solution groupe, firme spécialisée, tests réguliers, mesures de sécurité, …).

Il décrit également les grandes lignes du plan d'urgence en place qui doit lui permettre de fonctionner normalement en cas de panne de son système informatique, y compris pour ce qui est des connexions externes (recours à plusieurs fournisseurs de lignes de communication, redondance des lignes).

4. Rapports périodiques à communiquer

Le PSF de support doit décrire le système mis en place en vue d'établir les rapports prudentiels périodiques à envoyer à la CSSF ainsi que les mesures de contrôle interne visant à garantir que les données communiquées à la CSSF sont complètes, correctes et établies selon les règles qui s'y appliquent et transmises dans les délais imparties, y compris pour les chiffres définitifs.

5. Analyse des comptes annuels

Le PSF de support doit fournir une analyse des comptes annuels qui doit comprendre des commentaires et des explications spécifiques sur les postes importants et les évolutions remarquables de la situation financière.

A noter que pour ce point il ne faudra pas reproduire l'annexe des comptes annuels, mais fournir des informations et explications complémentaires pertinentes (exemples : justification de comptes d'un montant anormalement faible ou élevé dû par exemple à une activité de cash-pooling pour le groupe ; activité de consolidation européenne pour le groupe).

Le PSF de support mentionnera également les éléments postérieurs à la clôture qui sont de nature à avoir une influence sur l'appréciation de sa situation économique et financière.

6. Obligations professionnelles en matière de prévention du blanchiment et du financement du terrorisme

Le PSF de support doit fournir une description des procédures établies en vue de la prévention du blanchiment de capitaux et du financement du terrorisme[15] et notamment des procédures suivantes :

- « Know Your Customer » policy ;
- procédure de dénonciation de soupçon prédéfinie en interne ;
- procédure d'information au procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg et à la CSSF.

Le PSF de support précise également s'il a mis en place :

- un programme régulier de formation de ses employés ;
- la revue et la validation des procédures par la direction ;
- l'information et la communication de l'ensemble des procédures au sein du personnel du PSF de support ;
- la mise à disposition des procédures sur un support.

7. Obligations professionnelles en matière de règles de conduite

Le PSF de support devra donner une brève description de ses procédures internes pour l'application des règles de conduite et le traitement des réclamations de la clientèle.

8. Relations avec les entreprises liées

Le PSF de support s'engage à ce que les transactions intragroupes s'effectuent à des conditions de marché (« *at arm's length* »).

Sont à décrire et à commenter notamment :

- le type d'opérations intragroupes effectuées ;
- les garanties émises en faveur/reçues de la part d'entreprises liées ;
- les prix facturés pour services rendus et obtenus ;
- etc.

Toutes les transactions qui ne sont pas effectuées aux conditions de marché doivent être rapportées et détaillées.

15. Se référer au site internet de la CSSF (www.cssf.lu) à la rubrique « LBC/FT-Sanctions financières ».

9. Succursales à l'étranger

Le PSF de support fournit pour chaque succursale :

- un organigramme ;
- une description des activités ;
- une description des procédures de contrôle interne ;
- les déficiences graves que l'audit interne a relevées le cas échéant auprès de la succursale ;
- une description de l'organisation administrative et comptable ;
- une indication sur l'existence de procédures relatives au respect des règles de conduite et à la prévention du blanchiment et du financement du terrorisme ;
- des explications sur l'intégration comptable de la succursale.

10. Filiales à l'étranger

Le PSF de support devra fournir annuellement le rapport annuel ou, à défaut les comptes annuels des filiales ou participations majoritaires.

IV. Communication aux tiers

Le PSF de support est autorisé à communiquer à ses clients et prospects l'auto-évaluation de ses risques telle que définie au point II.B du chapitre II et les documents d'analyse s'y rapportant sous réserve de n'y apporter aucune modification et de les communiquer dans leur intégralité.

Alternativement, le PSF de support peut leur fournir une synthèse de son auto-évaluation sous réserve que celle-ci reflète toujours un profil de risques fidèle à celui se dégageant de l'auto-évaluation communiquée à la CSSF. Une copie de cette synthèse doit alors être transmise à la CSSF.

Dans tous les cas, le PSF de support veille à anonymiser les documents communiqués à ses clients et prospects.

Cette communication relève de la responsabilité exclusive du PSF de support qui s'engage quant à la véracité des informations communiquées. Le PSF de support ne peut en aucun cas se prévaloir d'une quelconque validation par la CSSF des documents et informations communiqués.

V. Dispositions finales et transitoires

La circulaire entre en vigueur à sa date de publication et portera initialement sur l'exercice 2012 pour les PSF de support clôturant au 31 décembre 2012.

Le premier rapport d'analyse de risques (« RAR ») est à remettre au plus tard 3 mois après la date de clôture, soit dès 2013. Les risques à inclure dans ce premier rapport sont :

a) conformément aux dispositions du chapitre II (point II.B) de la présente circulaire, les 20 risques directs et 5 risques indirects ayant obtenu les scores les plus élevés lors du calcul de l'importance nette (résultats les plus élevés des opérations (P_{nette} x $I_{net\ le\ plus\ élevé}$)). Toutefois, tout risque direct ou indirect dont l'impact net est égal ou supérieur à 6 tout en ayant simultanément une probabilité nette égale ou supérieure à 5 est également à rapporter, même si les limites de 20 et de 5 risques mentionnées ci-dessus sont par ailleurs atteintes ;

b) et, en sus, les 20 risques directs et 20 risques indirects les plus importants avant prise en compte des mesures de mitigation, quelle que soit par ailleurs l'importance nette de ces risques.

Dès le deuxième rapport d'analyse de risques et pour tous les suivants, les PSF de support rapporteront uniquement les risques visés au point a) ci-dessus, en conformité avec les dispositions du chapitre II (point II.B) de la présente circulaire.

Par ailleurs et pour rappel, tout événement survenant durant l'année et modifiant significativement le profil de risques au secteur financier du PSF (par exemple, apparition d'un nouveau risque significatif ou réévaluation à la hausse de l'importance d'un risque déjà identifié) doit être communiqué à la CSSF par le PSF de support, sans attendre l'émission du prochain rapport d'analyse de risques, sous la forme d'une fiche de risque telle que présentée au point II.B.

La CSSF encourage les PSF de support à préparer leur rapport d'analyse de risques au courant de l'année 2012. Durant cette année, ceux-ci pourront solliciter la CSSF pour discuter de leurs premiers éléments d'analyse de risques avant remise des rapports.

Le premier rapport descriptif (« RD ») est à remettre au plus tard 7 mois après la date de clôture 2012. Les années suivantes, le RD est à remettre en même temps que le RAR.

Pour rappel, les PSF de support doivent aussi communiquer spontanément à la CSSF et sans y être invités spécifiquement, les pièces relatives à leur clôture comptable. Dans tous les cas, les PSF de support ont un délai maximal de 7 mois[16] à partir de la date de clôture

16. En cohérence avec les articles 9 de la loi du 10 août 1915 sur les sociétés commerciales, 79 (1) de la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés, ainsi que la comptabilité et les comptes annuels des entreprises et 55 (2) de la LSF, qui imposent le dépôt au registre de commerce et des sociétés dans le mois de leur approbation, et au plus tard 7 mois après la clôture de l'année sociale, et la publication au Mémorial dans les deux mois du dépôt, des comptes annuels régulièrement approuvés.

de l'exercice pour envoyer à la CSSF les rapports et commentaires écrits émis par le réviseur d'entreprises agréé dans le cadre de son contrôle des documents comptables annuels[17].

Le tableau ci-dessous récapitule les délais accordés aux PSF de support pour fournir à la CSSF les documents attendus.

Documents à fournir	**En 2013**	**Après 2013 et avant l'entrée en vigueur de la seconde circulaire (Note 1)**	**A partir de l'entrée en vigueur de la seconde circulaire**
Rapport d'analyse de risques (RAR)	Au plus tard 3 mois après la clôture 2012	Au plus tard 3 mois après la clôture	Au plus tard 3 mois après la clôture
Rapport descriptif (RD) **(Note 2)**	Au plus tard 7 mois après la clôture 2012	Au plus tard 3 mois après la clôture	Au plus tard 7 mois après la clôture
Pièces relatives à la clôture comptable	Au plus tard 7 mois après la clôture 2012	Au plus tard 7 mois après la clôture	Au plus tard 7 mois après la clôture

Note 1 : Il s'agit de la seconde circulaire (étape 2) mentionnée en introduction. Elle viendra définir les règles pratiques concernant la mission des réviseurs d'entreprises agréés auprès des PSF de support et le contenu du compte rendu analytique de révision.

Note 2 : Les documents demandés dans la partie III de la présente circulaire[18] – tels que récapitulés ci-dessous - sont à annexer au rapport descriptif :

- un exemplaire du rapport sur les comptes annuels et des comptes annuels de l'actionnaire majoritaire direct ainsi que de son rapport de gestion lorsque ce dernier point est applicable ;
- le rapport écrit de la direction sur l'état du contrôle interne ;
- une copie du rapport de synthèse sur les contrôles effectués par l'audit interne au cours de l'exercice écoulé ;
- une copie de la ou des lettre(s) de mission confiée(s) à l'auditeur interne ;
- le plan pluriannuel d'audit interne entériné par la direction et/ou le conseil d'administration (ou conseil de gérance) ;
- la charte d'audit interne ;
- un tableau concernant les personnes désignées comme responsables de certaines fonctions en vertu des circulaires de la CSSF ;
- une liste à jour des membres de la direction en charge de la gestion journalière ;
- un tableau de synthèse des systèmes informatiques à usage interne ;
- une liste nominative des clients des secteurs financiers luxembourgeois ou étrangers pour lesquels le PSF de support preste des services nécessitant un agrément PSF ;

17. Conformément à l'article 54(1) de la LSF.
18. Se référer à la partie III pour des précisions sur le contenu attendu de ces documents.

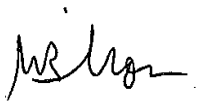
- la copie d'un contrat client portant sur des prestations de service nécessitant un agrément PSF, et ce pour chaque agrément PSF différent dont le PSF de support dispose ;
- un tableau de synthèse des systèmes informatiques à usage externe ;
- un schéma fonctionnel des flux ;
- le rapport annuel ou à défaut, les comptes annuels des filiales ou participations majoritaires.

Dès qu'il en a connaissance, le PSF de support informera la CSSF de tout retard annoncé en indiquant les raisons et la durée probable du retard.

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

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON
Directeur



Andrée BILLON
Directeur

Simone DELCOURT
Directeur

Jean GUILL
Directeur général

Annexe 1 : Echelles de probabilité et d'impact
Annexe 2 : Exemple de fiche de risque
Annexe 3 : Exemple de registre des risques directs et indirects au secteur financier
Annexe 4 : Exemple de tableau de synthèse des systèmes informatiques à usage interne
Annexe 5 : Exemple de tableau de synthèse des systèmes informatiques à usage externe

Annexe 1

Echelles de probabilité et d'impact

Echelle de probabilités

Valeur	Descriptif indicatif
0	Ne se produit pas / jamais
1	Ne se produit a priori pas / très improbable
2	Evènement isolé / rare
3	
4	Evènement répétitif / possible
5	
6	Evènement récurrent / probable
7	
8	Evènement courant / très probable
9	
10	Evènement constant / certain

Echelles d'impacts

- Impact sur la réputation

Valeur	Descriptif indicatif
0	Pas d'impact
1	
2	Rumeur(s), inquiétude de client(s) isolé(s)
3	
4	Couverture dans la presse nationale Nombreuses demandes d'informations de clients
5	
6	Couverture dans la presse spécialisée Perte de quelques clients ou d'un client stratégique
7	
8	Couverture dans tous les médias audio-visuels nationaux Départ massif de clients
9	
10	Couverture presse/médiatique internationale Départ de tous les clients

- Impact opérationnel

Valeur	Descriptif indicatif
0	Pas d'impact
1	
2	Incident(s) mineur(s) sans impact sur la clientèle
3	
4	Incident(s) isolé(s) avec impact(s) gérable(s) sur la clientèle
5	
6	Incident(s) isolé(s) avec impact(s) significatif(s) sur la clientèle / interruption d'un processus entier
7	
8	Incident(s) généralisé(s) avec impact(s) sur plusieurs clients / arrêt partiel des activités
9	
10	Arrêt complet des activités

- Impact légal

Valeur	Descriptif indicatif
0	Pas d'impact
1	
2	Rappel(s) CSSF Réclamation mineure / isolée de client(s)
3	
4	Lettre d'observation / demande de prise de position CSSF Dispute(s) commerciale(s) / constitution de provisions
5	
6	Manquement régulier - menace d'amende / Injonction CSSF Affaire au civil / litige client isolé
7	
8	Grave manquement - Amendes / Révocation Direction / Menace de retrait d'agrément CSSF Affaire au pénal / litiges clients massifs
9	
10	Perte / retrait de l'agrément CSSF Mise en cessation de paiement / liquidation de la société

- Impact financier

Valeur	Descriptif indicatif
0	Pas d'impact
1	
2	Perte(s) mineure(s)
3	
4	Perte(s) impactant modérément le résultat trimestriel
5	
6	Perte(s) impactant significativement le résultat de l'exercice
7	
8	Perte(s) majeure(s) annihilant le résultat de l'exercice en cours et/ou ceux ultérieurs
9	
10	Perte(s) majeure(s) et irrécouvrable(s) menaçant la pérennité de la société et/ou conduisant au dépôt de bilan

Annexe 2

Exemple de fiche de risque

Risque Id : 1	Catégorie : D6.1	Titre : Mutualisation - Ségrégation des environnements non assurée

Description du risque :
Dans un contexte de mutualisation, risque que la ségrégation des environnements clients ne soit pas assurée.

Evaluation brute (avant contrôles) :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
7	6	8	8	8	7*8 = 56

Argumentation :
Risque sur la confidentialité et l'intégrité des données clients, pouvant avoir des impacts opérationnels graves pour les clients et des impacts légaux (par ex. : secret professionnel non respecté) pour les clients et le PSF.

Clients secteur financier concernés :
Clients X, Y et Z concernés par l'offre mutualisée.

Mesures de diminution ou de transfert, et de suivi du risque :
- Duplication des instances applicatives sur un seul système d'exploitation.
- Robustesse technique du partitionnement : implémentation propre, documentée, régulièrement contrôlée, suivi des vulnérabilités et mises à jour correctrices régulières.

Evaluation nette (après contrôles) :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
1	6	8	8	8	1*8 = 8

Stratégie de réponse (y inclus argumentation si le choix est d'accepter le risque) : Réduire

Plan d'actions (y inclus échéances) :
Cryptographie des partitions au niveau du système d'exploitation (échéance : MM/AA)

Importance attendue :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
1	4	4	6	2	1*6 = 6

Risque Id : 12	Catégorie : I1	Titre : Des décisions imposées par le groupe mettent nos activités ou notre statut de PSF à risque

Description du risque :
Etant donné le contexte économique actuel, le groupe pourrait nous imposer une réduction d'effectif de 15% impactant principalement notre organisation interne et administrative et notre capacité à respecter les exigences réglementaires (administration centrale).

Evaluation brute (avant contrôles) :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
7	6	4	8	6	7*8 = 56

Argumentation :
Risque de réputation et de perte de parts de marché, risque de non-conformité à la réglementation. Indirectement pour nos clients, risques opérationnels.

Clients secteur financier concernés :
Tous les clients.

Mesures de diminution ou de transfert, et de suivi du risque :
Actions de sensibilisation du groupe au statut de PSF de support et obligations y relatives.

Evaluation nette (après contrôles) :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
6	6	4	8	6	6*8 = 48

Stratégie de réponse (y inclus argumentation si le choix est d'accepter le risque) : Réduire

Plan d'actions (y inclus échéances) :
Poursuivre les actions de sensibilisation (échéance : MM/AA) ; s'accorder sur une politique de gouvernance avec le groupe (échéance : MM/AA).

Importance attendue :

Probabilité (P)	Impacts (I)				Importance ($PxI_{le\ plus\ élevé}$)
	Réputation	Opérationnel	Légal	Financier	
4	6	4	8	6	4*8 = 32

Annexe 3

Exemple de registre des risques directs et indirects au secteur financier

Cat.	ID.	Titre du risque	Evaluation brute			Evaluation nette			Stratégie de réponse
			P	I	Imp.	P	I	Imp.	Stratégie de réponse
Risques directs									
D6.1	1	Mutualisation - Ségrégation des environnements non assurée	7	8	56	1	8	8	Réduire
…	…	…							…
D5	5	…							Accepter
…	…	…							…
Risques indirects									
I1	12	Des décisions imposées par le groupe mettent nos activités ou notre statut de PSF à risque	7	8	56	6	8	48	Réduire
…	…	…							

Annexe 4

Exemple de tableau de synthèse des systèmes informatiques à usage interne

<table>
<tr><th>Fonction</th><th>Eléments logiciels</th><th>Eléments matériels physiques</th><th>Eléments matériels virtuels</th></tr>
<tr><td rowspan="2">FONCTION PSF :
• COMPTABILITE GENERALE (fonction sous-traitée au groupe)</td><td>NOM DU LOGICIEL (et fournisseur si progiciel) :

Développement : interne, progiciel (moins de 20% d’adaptations du produit standard), mixte
Modifications depuis l’exercice précédent :</td><td>Marque :
Modèle : PC
OS (operating system) : nom et version
Mode de redondance : Cold standby
Raison redondance : Criticité faible (48H d’arrêt max)
Nombre : 2
Identification : PC01, PC02
Machine Virtuelle (MV) : 2 VM par élément</td><td>Type de MV : VMware
OS (operating system) : nom et version
Nombre : 4
Identification et hébergement :
VM01 et VM02 sur PC01
VM03 et VM04 sur PC02</td></tr>
<tr><td colspan="3">Outsourcing : oui, hébergement de l’infrastructure physique à la maison-mère aux USA et administration des VM et du logiciel par une société sœur au UK
Dédié/partagé : Logiciel mutualisé avec d’autres entités du groupe (mode Multiple Entities Single Instance). Eléments matériels physiques et virtuels partagés avec d’autres entités du groupe.
Opéré par : maison-mère (matériels physiques) et société sœur au UK (VM et logiciel)
Localisation : Los Angeles, USA, maison-mère
Existence d’un plan de reprise : oui, reprise en interne (conditions inclues dans le contrat avec le groupe)</td></tr>
<tr><td rowspan="2">FONCTION TECHNIQUE :
• FIREWALL</td><td>NOM DU LOGICIEL :

« trusted OS »</td><td>Marque :
Modèle : PC
OS (operating system) : nom et version
Mode de redondance : Clustering
Raison redondance : Criticité (1 min d’arrêt max)
Nombre : 1
Identification : FW1
MV : N/A</td><td>N/A</td></tr>
<tr><td colspan="3">Outsourcing : non
Dédié/partagé : dédié
Opéré par : le PSF de support
Localisation : Locaux du PSF
Existence d’un plan de reprise : N/A</td></tr>
</table>

Annexe 5

Exemple de tableau de synthèse des systèmes informatiques à usage externe

<table>
<tr><th>Fonction</th><th>Eléments logiciels</th><th>Eléments matériels physiques</th><th>Eléments matériels virtuels</th></tr>
<tr><td rowspan="2">FONCTION CLIENT :
• COMPTABILITE DE FONDS</td><td>NOM DU LOGICIEL (et fournisseur si progiciel) :

Gestion des données : type et nom du produit SGBD
Analyse et programmation : type (Classique, Orienté Objet, mixte) et nom des langages et/ou des outils CASE
Mode : Transactionnel temps réel, batch, mixte
Architecture : simple ou client-serveur avec nombre de niveaux (2, 3 ou plus) et lien avec le matériel utilisé
Développement : interne, progiciel (moins de 20% d’adaptations du produit standard), mixte
Modifications depuis l’exercice précédent :</td><td>Marque :
Modèle :
OS (operating system) : nom et version
Mode de redondance :
Raison redondance :
Nombre : 2
Identification : PC01, PC02
MV : 2 VM par élément
Nombre total de clients :
- Sur PC01 :
- Sur PC02 :
Nombre de clients secteur financier :
- Sur PC01 :
- Sur PC02 :</td><td>Type de MV : VM
OS (operating system) : nom et version
Nombre : 4
Identification et hébergement :
VM01 et VM02 sur PC01
VM03 et VM04 sur PC02</td></tr>
<tr><td colspan="3">Outsourcing : oui, hébergement et opération de l’infrastructure (physique et virtuels) à un PSF de type OSIP (à nommer).
Dédié/partagé : Logiciel dédié au PSF de support et proposé à ses clients en mode Saas. Eléments matériels physiques et virtuels mutualisés (mode Iaas).
Opéré par : logiciel opéré par le PSF de support. Infrastructure opérée par le PSF OSIP.
Localisation : Locaux du PSF OSIP.
Existence d’un plan de reprise : oui, transfert à un autre prestataire (conditions inclues dans le contrat avec le prestataire actuel)</td></tr>
</table>