Luxembourg, le 22 mars 2006

A tous les établissements de crédit et autres professionnels du secteur financier

CIRCULAIRE CSSF 06/240
telle que modifiée par les circulaires CSSF 13/568 et CSSF 17/657

Concerne : Organisation administrative et comptable; sous-traitance en matière informatique et précisions concernant les services relevant d'un agrément de PSF de support, articles 29-1, 29-2, 29-3, 29-4, 29-5 et 29-6 de la loi modifiée du 5 avril 1993 sur le secteur financier (LSF)

Mesdames, Messieurs,

La présente circulaire a pour objet de préciser les modalités d'application de l'article 5(2) de la loi du 5 avril 1993 relative au secteur financier (ci-après désignée par « la loi ») pour les banques et de l'article 17(2) de la loi pour les professionnels du secteur financier (ci-après désignés par PSF) lorsqu'un professionnel financier fait appel à un tiers pour des services susceptibles de requérir un agrément de PSF de support selon les articles 29-1, 29-2, 29-3, 29-4, 29-5 et 29-6 de la loi.

Les précisions portent sur :

- les responsabilités du professionnel financier en matière de confidentialité lorsqu'il s'adresse à un PSF de support pour des services autres que ceux requérant un agrément,
- la délimitation entre le statut d'opérateur de systèmes informatiques et de réseaux de communication du secteur financier (ci-après désigné par « OSIP pour l'article 29-3 et OSIS pour l'article 29-4 ») tel que défini aux articles 29-3 et 29-4 de la loi et celui d'agent administratif défini à l'article 29-2 de la loi,
- les activités qui relèvent du statut d'OSIP et d'OSIS,
- le bon usage de la prestation d'intérimaire pour des fonctions-clés informatiques,
- les prestations informatiques, en complément « des circulaires CSSF 17/656[1] et CSSF 12/552 »[2], de migration d'infrastructure et de données, ainsi que d'assistance aux utilisateurs (help desk),

[1] Abroge et remplace la circulaire CSSF 05/178
[2] Circulaire CSSF 13/568

- les fonctions de gestion de courrier et d'assistance à la clientèle,

1. <u>Les responsabilités du professionnel financier en matière de confidentialité, lorsqu'il recourt à un PSF de support pour des services autres que ceux requérant un agrément</u>

   1.1. Le professionnel financier peut vouloir recourir à des prestataires disposant d'un statut de PSF de support pour des prestations qui ne relèvent pas d'un agrément.

   L'article 41(5) de la loi indique que l'obligation au secret professionnel n'existe pas « …dans la mesure où les renseignements communiqués à ces professionnels sont fournis dans le cadre d'un contrat de services relevant de l'une des activités réglementées par les dispositions légales susmentionnées et à condition que ces renseignements soient indispensables à l'exécution du contrat de services en cause. ». Il est donc important pour le professionnel financier de savoir si cette absence d'obligation s'applique à l'intégralité des services prestés par les PSF de support disposant d'un statut selon les articles 29-1, 29-2, 29-3, 29-4, 29-5 et 29-6 de la loi, c'est-à-dire s'il a le droit de confier à ces prestataires des travaux soumis au secret professionnel autres que ceux liés à l'opération de systèmes informatiques ou de réseaux de communication.

   Etant donné que les articles 29-3 (2) et 29-4 (2) énoncent que « les opérateurs de systèmes informatiques … sont habilités à effectuer également la mise en place et la maintenance des systèmes informatiques et des réseaux… », et afin d'éviter au professionnel financier toute ambiguïté relative au secret professionnel en relation avec la nature de la prestation, il convient de préciser que l'entièreté des services fournis par le PSF disposant du statut d'OSIP ou d'OSIS ne fera pas l'objet d'une obligation au secret professionnel de la part des professionnels financiers.

   Ainsi, le professionnel financier s'adressant à un PSF de support OSIP ou OSIS ne doit plus veiller à ce que le personnel du PSF de support intervenant sur site soit accompagné tout au long de sa mission par une personne du professionnel financier en charge de l'informatique.

   1.2. Alors que le recours à des PSF de support est obligatoire pour des activités qui relèvent d'un agrément, le professionnel financier disposera néanmoins du libre choix d'opter pour une sous-traitance auprès d'un PSF de support pour d'autres services. Lorsque le professionnel financier opte pour un PSF de support, toutes les prestations sont réalisées dans le cadre légal et réglementaire applicable au secteur financier. Les professionnels financiers ne sauraient toutefois exiger de leurs prestataires d'obtenir un agrément PSF de support alors que ceux-ci ne prestent aucune activité leur permettant d'obtenir cet agrément. Ainsi, un professionnel financier ne peut exiger de son prestataire d'avoir un agrément d'OSIP ou d'OSIS si celui-ci ne fournit

localement auprès du secteur financier que des services de développement ou de vente de matériel.

2. <u>Délimitation entre les statuts d'opérateur de systèmes informatiques et de réseaux de communication du secteur financier (OSIP ou OSIS) et d'agent administratif</u>

Ce chapitre présente le mode de raisonnement qui permet de définir si la prestation relève du statut d'OSIP ou d'OSIS ou de celui d'agent administratif. Le point 2.5. précise dans quel cas l'agent administratif doit cumuler le statut d'OSIP ou d'OSIS.Il revient aux professionnels financiers devant respecter les conditions de la circulaire CSSF 17/656 « ou de la circulaire CSSF 12/552 »[3] ou de la circulaire CSSF 17/654 relative au « cloud computing », de contracter au Luxembourg, pour des services d'opérations de systèmes informatiques OSIP ou OSIS tels que définis au chapitre 3 de la présente circulaire, avec des sociétés disposant de l'agrément adéquat.

2.2. Afin de déterminer si une prestation de services requiert le statut d'OSIP ou d'OSIS ou d'agent administratif, le professionnel financier devra au préalable évaluer si les services qu'il entend sous-traiter s'étendent au-delà de la prestation purement technique d'opération des systèmes. Si ces services portent sur des tâches pouvant impacter l'activité du professionnel financier, à savoir par exemple la saisie d'informations financières pour lesquelles une erreur aurait un impact sur l'activité, l'agrément d'OSIP ou d'OSIS ne sera pas suffisant et le professionnel devra s'orienter vers une société disposant également du statut d'agent administratif tel que décrit à l'article 29-2 de la loi.

2.3. L'injection de données fournies sous forme de fichiers par un tiers ou par le professionnel financier, est à voir comme une tâche technique liée aux interfaces des systèmes dès lors qu'il n'y a aucune intervention humaine sur les données de la part du prestataire. Ainsi, par exemple, un fichier contenant des cours boursiers ou de change peut être injecté dans les applications à condition que le prestataire n'apporte aucune appréciation sur l'exactitude des cours. Afin que la prestation reste de nature technique, les données ne peuvent être modifiées que par un traitement informatique, en accord avec le professionnel financier qui doit en comprendre les effets, et non par intervention manuelle du prestataire.

2.4. Le paramétrage technique des systèmes ou des applications, tel que l'attribution des droits d'accès aux utilisateurs, peut néanmoins être considéré comme relevant uniquement du statut d'OSIP ou d'OSIS, à condition que la définition des droits d'accès soit sous le contrôle du professionnel financier.

2.5. Un professionnel financier peut contracter avec un agent administratif pour la prise en charge d'un ensemble d'activités qui sont supportées par l'informatique. Tant que le prestataire ne met pas directement sa plateforme informatique à disposition du professionnel financier en dehors des services administratifs prestés, c'est-à-dire que cette plateforme n'est utilisée que par le prestataire dans le cadre des services réalisés comme agent administratif, ceci même si le professionnel financier y a des accès, la prestation ne constitue pas une activité d'opération nécessitant le statut d'OSIP ou d'OSIS, mais elle

[3] Circulaire CSSF 13/568

requiert uniquement le statut d'agent administratif. Ainsi, il est également possible pour un agent administratif disposant de l'agrément 29-2 selon la loi, de recourir à des services de « cloud computing » au sens de la circulaire CSSF 17/654, dès lors que ces services de cloud ne sont pas directement fournis au professionnel financier en dehors de la prestation de services administratifs. L'agent administratif devra cependant respecter les conditions de la circulaire CSSF 17/654 sur le « cloud computing », en qualité de « ESCR » (établissement surveillé par la CSSF et consommant des ressources de cloud computing). Si, par contre, le prestataire met à disposition un équipement informatique qu'il administre, mais qui ne sert pas à son activité d'agent administratif, alors le statut d'OSIP ou d'OSIS devient obligatoire car la prestation n'est plus de la même nature.

3. Qualification de la prestation technique sous-traitée en vue de déterminer si elle relève d'un agrément OSIP ou OSIS

   3.1. Lorsqu'une prestation technique ne relève pas d'une sous-traitance de nature informatique reposant sur une infrastructure de cloud computing telle que définie dans la circulaire 17/654, elle sera considérée comme constituant une activité d'opération à partir du moment où :

      3.1.1. La prestation porte sur un équipement situé dans un environnement de production, ce qui inclut le parc bureautique composé de postes de travail et de serveurs d'impression ou de stockage

   et qu'au moins un des deux critères suivants est rempli :

      3.1.2. La responsabilité du bon fonctionnement de cet équipement ou d'une application qui y est logée est explicitement définie par contrat ou le professionnel financier a de fait perdu le contrôle et les connaissances de l'équipement ou de l'application pour lequel intervient le prestataire.

      3.1.3. Le prestataire intervient sur cet équipement ou cette application, sans que le professionnel financier n'en ait toujours connaissance. Ceci est en particulier le cas lorsque le prestataire dispose d'un accès à distance non contrôlé ou lorsqu'il est physiquement présent dans les locaux mais que ses actions et interventions sur les systèmes sont insuffisamment contrôlées par le professionnel financier.

   3.2. Lorsqu'une prestation technique relève d'une sous-traitance de nature informatique reposant sur une infrastructure de cloud computing telle que définie dans la circulaire 17/654, elle sera considérée comme constituant une activité d'opérations à partir du moment où elle répond à la définition d'opération de ressources de cette circulaire CSSF 17/654.

   3.3. Activités ne relevant pas d'un agrément OSIP ou OSIS

      3.3.1. Les activités de fourniture de cloud au sens de la circulaire CSSF 17/654.

      3.3.2. En principe, le professionnel financier peut recourir à du personnel externe ne faisant pas partie d'un PSF de support pour l'assister dans des tâches sur ses systèmes de production susceptibles de contenir des

données confidentielles[4]. Il doit alors veiller à limiter autant que possible les accès occasionnels aux données confidentielles réellement nécessaires à l'exécution des tâches et doit s'assurer, au moyen d'un document à signer, que ce personnel a connaissance de l'obligation au secret professionnel qui lui incombe au titre de l'article 41 de la loi lorsqu'il est au service de la banque. Le professionnel financier informera notamment ce personnel des poursuites pénales encourues en cas de manquement à cette obligation au secret.

3.3.3. La fourniture, l'installation et la configuration de matériel informatique ne relèvent pas de l'agrément OSIP ou OSIS, à condition que la prestation ne soit pas suivie d'une prise en charge dépassant le simple cadre d'une maintenance corrective ou adaptative.

3.3.4. Il en est de même pour le développement d'applications, l'assistance, le conseil et la maintenance qui ne nécessitent pas d'agrément, à condition toutefois que la prestation n'inclue pas un service de support déchargeant le professionnel financier des tâches d'exploitation ou d'administration des systèmes ou des applications fournies.

3.3.5. La surveillance d'équipements et d'applications (monitoring) ne relève pas d'un agrément OSIP ou OSIS lorsque le professionnel financier intervient suivant les instructions données par le prestataire pour agir sur les systèmes surveillés et que le prestataire ne dispose jamais des moyens d'intervenir de son propre chef.

3.4. Il appartient au professionnel financier de déterminer et de vérifier par après, pour chaque prestation de nature informatique qu'il entend sous-traiter ou qu'il a déjà sous-traitée, si celle-ci relève de l'activité d'opération de systèmes et de réseaux.

4. <u>La prestation d'intérimaire</u>

4.1. Par prestation d'intérimaire, au sens de la présente circulaire, il faut comprendre la mise à disposition par un prestataire de personnes disposant de compétences spécifiques et qui sont rémunérées par le prestataire. Le contrat de service est donc bien conclu entre le professionnel financier et le prestataire qui met à disposition le personnel qualifié. Par contre, la simple mise en relation de personnes qualifiées en vue de la réalisation d'un travail intérimaire pour compte du professionnel financier ne relève pas de la prestation d'intérimaire au sens de la présente circulaire, lorsque celles-ci sont engagées et rémunérées par le professionnel financier.

4.2. En cas de recours à du personnel intérimaire, les tâches à réaliser sont clairement définies par le professionnel financier et la responsabilité du

[4] Seuls les systèmes de production sont supposés contenir des données confidentielles. Les systèmes de développement et de tests ne devraient pas en contenir.

prestataire se limite à proposer un personnel aux compétences définies dans le contrat.

4.3. Le personnel intérimaire est à considérer par le professionnel financier comme un tiers au sens des circulaires CSSF 17/656 et CSSF 12/552.

4.4. Un professionnel financier peut recourir à une prestation d'intérimaire, mais il doit rester attentif à garder les compétences et les connaissances suffisantes pour garantir la pérennité de ses activités. Ceci est particulièrement vrai lorsque le professionnel financier recourt systématiquement à du personnel temporaire pour des fonctions clés des activités informatiques liées aux environnements de production, notamment en raison des risques potentiels d'une dilution des connaissances du professionnel financier sur le long terme, d'une moindre contribution au développement d'une culture d'entreprise spécifique au professionnel financier et au secteur financier ainsi que d'une possible déresponsabilisation de ce personnel.

4.5. Le professionnel financier fera preuve de prudence pour les fonctions informatiques d'opérations de ressources au sens de la circulaire CSSF 17/654 portant sur le « cloud computing », d'administration de systèmes, de réseaux ou de bases de données confiées à du personnel intérimaire lorsque les travaux sont réalisés sur des équipements de production et non sur des équipements de développement ou de tests. Ces fonctions impliquent souvent d'importantes responsabilités, en particulier parce qu'elles permettent au personnel qui y est affecté, une manipulation complète des systèmes gérés ou l'accès sans restrictions aux données stockées dans les bases, ceci en raison des droits d'accès de plus haut niveau dont ce personnel dispose pour accomplir sa mission.

4.6. Lorsque ces fonctions d'administration sur des systèmes de production sont confiées à du personnel temporaire, il est impératif pour le professionnel financier de ne pas se trouver dans une situation de dépendance vis-à-vis de celui-ci. Ainsi, le professionnel financier veillera à limiter la durée de la prestation au strict nécessaire, le temps pour lui de procéder au recrutement du personnel chargé de reprendre les fonctions réalisées par le personnel temporaire, ou de confier la sous-traitance de ces fonctions à un PSF disposant du statut d'OSIP ou OSIS.

5. <u>La migration de systèmes et de données</u>

5.1. Il convient de discerner les projets de migration spécifiques aux systèmes de ceux spécifiques aux données.

5.1.1. Les projets de migration de systèmes

Concernant la migration de systèmes, les données, qu'elles soient de nature confidentielle ou non, ne constituent pas le cœur du projet. Le personnel affecté à la migration dispose d'une expertise spécifique de l'ancien ou du nouveau système.

Dans la mesure où la migration des données de ce type de projet implique peu d'interventions manuelles sur ces données en comparaison aux processus automatiques de migration qui sont développés, et partant du principe que l'accès aux données confidentielles est limité et semblable à

celui rencontré dans des projets de mise en production d'applications informatiques, le professionnel financier pourra appliquer le principe de la circulaire CSSF 17/656 « (repris dans la circulaire CSSF 12/552) »[5] qui indique que le prestataire intervenant dans un environnement de production susceptible de contenir des données confidentielles, doit être accompagné tout au long de sa mission par une personne du professionnel financier en charge de l'informatique. Il n'y a donc pas lieu de faire systématiquement appel à un PSF de support pour ce type de mission.

5.1.2. Les projets de migration de données

Il s'agit de prestations qui portent essentiellement sur le traitement des données et qui impliquent une manipulation humaine des données, combinée à une expertise sur celles-ci. L'exemple le plus classique consiste en l'archivage et l'indexation de documents. L'archivage suppose le plus souvent une manipulation des documents physiques à des fins de numérisation et l'indexation documentaire requiert une expertise du prestataire sur ces données indexées.

Dans ces deux cas de figure, le prestataire est amené à voir de façon massive les données traitées et la confidentialité devient un enjeu particulier qui impose le recours à un PSF de support puisque le professionnel financier ne peut déléguer des tâches donnant accès à des données confidentielles concernant ses clients qu'aux seuls professionnels pour lesquels la loi prévoit une exception au secret professionnel. En conséquence, le professionnel financier doit, pour tout projet de migration de données concernant des données confidentielles, s'adresser à un PSF de support. De plus, le professionnel financier devra déterminer si la manipulation de ces données, telle l'indexation, peut avoir des conséquences directes sur son activité. En cas de réponse positive, la prestation devra être confiée à un PSF disposant du statut d'agent administratif ou d'un statut de PSDC (articles 29-5 et 29-6 de la LSF) lorsqu'il s'agit d'archivage à valeur probante. Le statut d'OSIP ou d'OSIS ou d'agent de communication à la clientèle qui inclut les prestations d'archivage, ne suffit pas dans ce cas.

6. <u>Assistance aux utilisateurs (help desk)</u>

6.1. Il existe deux catégories d'assistance aux utilisateurs : l'assistance sans prise de contrôle et l'assistance avec prise de contrôle à distance ou paramétrage.

6.2. La première catégorie ne relève pas d'un agrément d'OSIP ou d'OSIS dans la mesure où les actions faites sur les systèmes sont réalisées par le personnel du professionnel financier sur base des indications faites par le prestataire qui ne dispose pas des accès sur ces systèmes.

6.3. La seconde catégorie consiste en une assistance par le prestataire avec prise de contrôle ou paramétrage du système du professionnel financier. Dans ces conditions, le prestataire peut opérer le système à distance et l'activité relève du statut d'OSIP ou d'OSIS, voire du statut d'agent administratif si le prestataire peut modifier à distance des données liées à l'activité du

[5] Circulaire CSSF 12/552

professionnel financier. Il en est ainsi notamment pour le cas d'une fonction de 'help desk' d'une application bancaire, avec prise de contrôle à distance par le prestataire de l'écran du personnel du professionnel financier ayant demandé assistance. D'une part, la présence de la personne assistée n'est plus impérative une fois la session initiée, d'autre part le prestataire dispose de la prise de contrôle de l'application au nom de la personne assistée et peut modifier la transaction en cours, voire en initier de nouvelles. Au-delà du problème de confidentialité que pose cette visualisation à distance, il existe le risque d'immixtion dans les activités du professionnel financier de la part du prestataire, avec les risques sous-tendus d'erreur ou de fraude.

6.4. L'assistance avec prise de contrôle, réalisée par un fournisseur de services de cloud computing au sens de la circulaire CSSF 17/654 n'est permise qu'en appui et sous contrôle de l'opérateur de ressources et non directement à l'ESCR[6]. En effet, l'opérateur de ressources est alors garant de l'intervention réalisée pour l'ESCR.

7. Gestion du courrier et assistance (help desk) à la clientèle

7.1. Lorsque le professionnel financier confie la gestion du courrier entrant ou sortant à un sous-traitant ou lorsqu'il fait appel à un sous-traitant pour un service d'assistance à la clientèle (call center ou help desk), il encourt un risque élevé de divulgation de l'identité des clients et il est impératif que le sous-traitant garde le secret sur les informations obtenues. En vertu de l'article 41(5), le professionnel financier n'est pas en droit de confier des tâches qui donnent accès à des données confidentielles à un prestataire de service qui ne dispose pas d'un agrément de PSF de support et en particulier d'un agrément d'agent de communication à la clientèle.

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

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT
Directeur

Jean-Nicolas SCHAUS
Directeur général

[6] Ces termes sont à comprendre au sens de la circulaire CSSF 17/654.