Commission de Surveillance du Secteur Financier

Version du 27 mars 2019

FAQ de la circulaire cloud computing

Foire aux questions : circulaire cloud computing

<u>Avertissement</u> : Cette « Foire aux Questions » (ci-après « FAQ ») a pour seul objectif d'aider les entités surveillées à répondre aux exigences de la circulaire CSSF 17/654, relative à la sous-traitance informatique reposant sur une infrastructure informatique en nuage ou infrastructure de « cloud computing » (« circulaire cloud computing »). Elle a été rédigée dans l'état actuel des connaissances de la CSSF et pourra être mise à jour en fonction des évolutions technologiques et des analyses futures de la CSSF. Les termes utilisés et définis dans la circulaire CSSF 17/654 ont la même signification dans cette FAQ.

QUESTION 1 : Lorsque plusieurs technologies de cloud computing sont utilisées par un opérateur des ressources (soit auprès d'un seul fournisseur de services de cloud computing, soit auprès de plusieurs), est-il nécessaire d'avoir un seul cloud officer ?

Mise à jour le 27 mars 2019

La circulaire n'impose pas nécessairement d'avoir un seul cloud officer. L'opérateur des ressources peut attribuer les responsabilités à plusieurs cloud officers comme il lui convient du moment qu'il est à même de démontrer qu'ils disposent globalement de la compétence requise pour chacun des clouds utilisés (par exemple, par modèle de services (SaaS, PaaS et IaaS) ou par produit de fournisseur de services de cloud computing). Il est également possible de définir une hiérarchie au sein des cloud officers. Dans tous les cas, dans le cadre de la communication à la CSSF des noms des cloud officers (cf. point 26 de la circulaire), il convient de fournir une brève explication du partage des responsabilités parmi les cloud officers.

QUESTION 2 : Les réseaux sociaux, qui reposent sur une infrastructure de cloud computing en mode SaaS (par exemple, Facebook, Twitter, LinkedIn, etc.), sont-ils soumis aux exigences de la circulaire cloud computing ?

Date de publication : 17 mai 2017

La circulaire s'applique aux sous-traitances sur une infrastructure de cloud computing. Si les réseaux sociaux sont utilisés pour des activités qui ne pourraient pas être internalisées, alors leur utilisation n'est pas considérée comme un cas de sous-traitance. Par exemple, les utilisations à des fins de communication externe (pour marketing, démarchage, etc.) ou pour usage privé ne sont pas considérées comme des cas de sous-traitance. A contrario, l'utilisation comme service de messagerie interne est considérée comme un cas de sous-traitance.

QUESTION 3 : Pouvez-vous donner des exemples d'activités considérées comme matérielles ?

Mise à jour le 27 mars 2019

La circulaire mentionne que l'ESCR doit détailler pourquoi il considère l'activité à sous-traiter sur une infrastructure de cloud computing comme matérielle ou non. C'est à l'ESCR de faire sa propre analyse et de la justifier. Néanmoins, certaines activités sont forcément à considérer comme matérielles par l'ESCR, comme par exemple l'utilisation d'un logiciel comptable ou l'utilisation d'un progiciel supportant le cœur de l'activité. A contrario, il est concevable que certaines activités soient considérées non matérielles par l'ESCR, comme par exemple l'hébergement d'environnements de tests ou le stockage d'informations publiques. Il convient de se référer au document « Frequently Asked Questions on the assessment of IT outsourcing materiality».

QUESTION 4 : Au point 30.f. de la circulaire, il est écrit que « *les fonctions de contrôle interne de l'ESCR doivent avoir un accès adapté aux données et systèmes, nécessaires à l'exercice de leurs missions, qui sont hébergés sur l'infrastructure de cloud computing* ». De quels données et systèmes parle-t-on ?

Date de publication : 17 mai 2017

Il s'agit des données et systèmes mis à disposition sur l'interface client et permettant aux fonctions de contrôle interne d'exercer leurs missions. Par exemple : les outils traçant les accès des utilisateurs, les outils fournissant des métriques quant aux paramètres de sécurité implémentés, la liste des utilisateurs ayant accès aux données et systèmes, etc.

QUESTION 5 : Certains fournisseurs de services de cloud computing proposent un contrat spécifique au secteur financier. Si tel est le cas, le signataire est-il contraint de signer ce contrat ou est-il libre de signer un autre contrat ?

Date de publication : 17 mai 2017

Il est de la responsabilité du signataire potentiel de demander systématiquement au fournisseur de services de cloud computing s'il existe un contrat spécifique au secteur financier. Le signataire potentiel doit ensuite évaluer si ce contrat répond aux exigences de la circulaire.

QUESTION 6 : Le point 27.a. de la circulaire mentionne la nécessité pour le cloud officer, l'audit interne et le responsable de la sécurité des systèmes d'informations de suivre des formations appropriées sur la gestion et la sécurité des ressources de cloud computing spécifiques au fournisseur de services de cloud computing. Quel est le formalisme à adopter pour répondre à cette exigence (ex. examen, certification) ?

Date de publication : 17 mai 2017

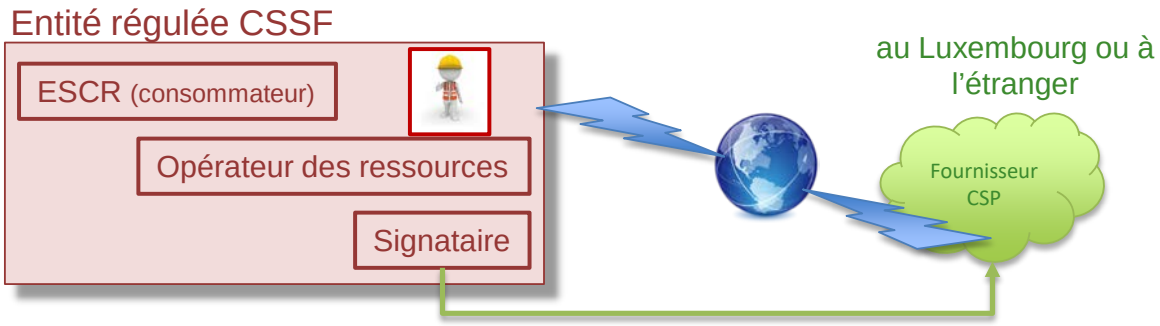
Il n'est pas exigé que les personnes ayant suivi des formations passent un examen ou obtiennent une certification. Néanmoins, il est nécessaire de conserver une attestation prouvant que la formation a été effectivement suivie à une date précise et listant précisément le contenu de la formation. Il est à noter que cette attestation peut être demandée à tout moment par la CSSF. L'opérateur des ressources veillera à garder à jour les compétences du cloud officer, de l'audit interne et du responsable de la sécurité des systèmes d'informations via des formations régulières.

QUESTION 7 : Pouvez-vous donner des exemples concrets d'attribution des rôles entre ESCR, opérateur des ressources et signataire ?

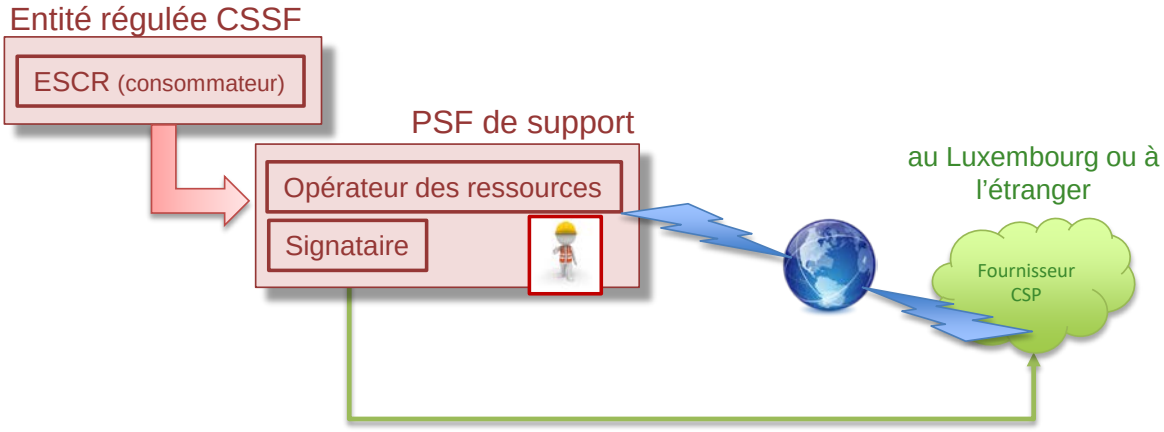
Date de publication : 17 mai 2017

Plusieurs scénarii sont envisageables pour l'attribution des rôles d'ESCR, d'opérateur des ressources et de signataire.

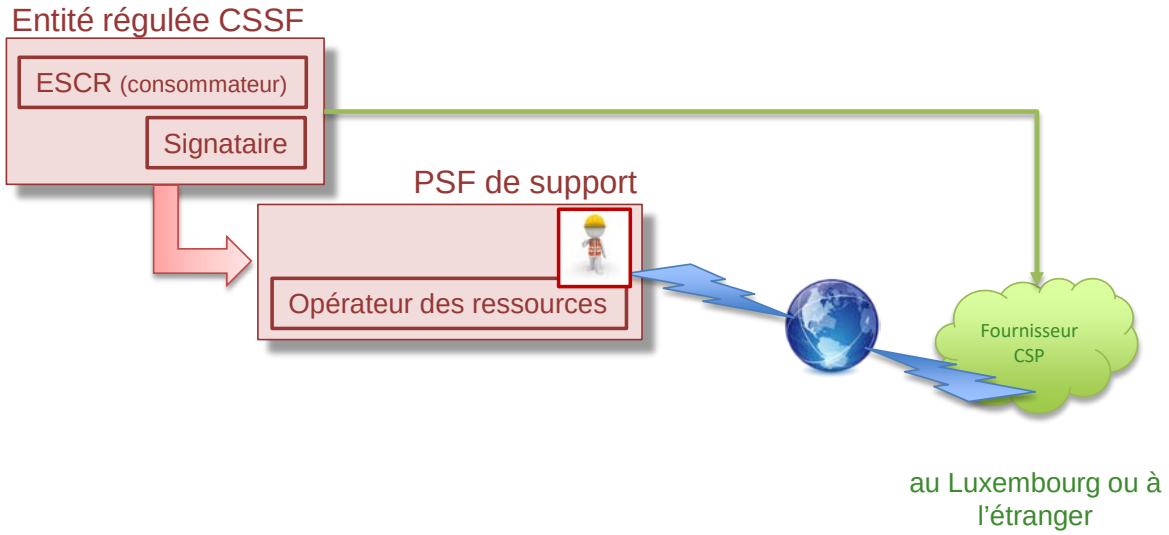
1) Le cas le plus simple étant le cumul de ces trois fonctions par l'entité surveillée par la CSSF. Le cloud officer se trouve ainsi au sein de cette entité.



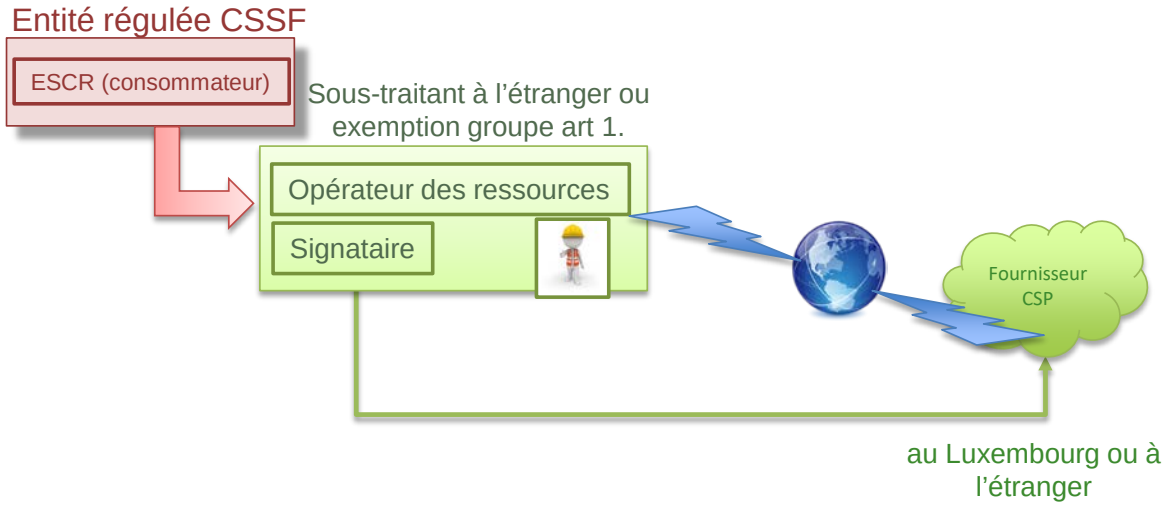
2) Un deuxième cas est une entité surveillée qui utilise un PSF de support en tant qu'intermédiaire. Le PSF de support serait à la fois opérateur des ressources et signataire. Le cloud officer se trouve ainsi au sein du PSF de support.



3) Un troisième cas est l'utilisation d'un PSF de support par l'ESCR seulement pour l'opération des ressources. L'entité surveillée cumule les fonctions d'ESCR et de signataire. Le cloud officer se trouve à nouveau au sein du PSF de support.
L'opérateur des ressources n'est pas responsable de la qualité du fournisseur mais peut fournir l'expertise nécessaire au consommateur qui doit, en qualité de signataire, s'assurer du bon choix et de la conformité du fournisseur.



4) L'ESCR peut faire appel pour l'opération des ressources à un sous-traitant ne bénéficiant pas d'un statut PSF de support, soit lorsque le sous-traitant est à l'étranger (faisant partie ou non du groupe de l'ESCR), soit lorsqu'il est basé au Luxembourg mais qu'il fait partie du groupe de l'ESCR et qu'il traite exclusivement des opérations du groupe (exemption prévue à l'article 1 de la LSF). Ce sous-traitant peut être signataire. L'ESCR doit s'assurer que l'opérateur de ressources répond aux exigences de la circulaire cloud computing et a lui-même fait son *due dilligence* sur le fournisseur selon les éléments de la circulaire cloud computing.



QUESTION 8 : Si une banque ou une entreprise d'investissement procède à une sous-traitance informatique qui tombe dans le périmètre de la circulaire cloud computing, la circulaire CSSF 12/552 ne lui est-elle plus applicable ?

Date de publication : 17 mai 2017

Seul le sous-chapitre 7.4 Sous-traitance ("outsourcing") de la circulaire CSSF 12/552 n'est dans ce cas plus applicable car il est remplacé par les exigences de la circulaire cloud computing. L'ensemble des exigences se trouvant dans les autres chapitres et sous-chapitres de la circulaire CSSF 12/552 restent d'application, notamment le point 17 dans le contexte d'une sous-traitance qui nous occupe ici.

QUESTION 9 : Quelles formations doivent être suivies par les cloud officers ?

Date de publication : 27 mars 2019

La CSSF n'a pas référencé et ne référencera pas de formations pour les cloud officers, d'autant qu'il existe un nombre croissant de solutions clouds, principalement d'applications en mode SaaS, mais également des solutions PaaS ou IaaS. En effet, nous considérons qu'il est de la responsabilité des entités surveillées d'évaluer les besoins en formation et de maintenir les compétences des cloud officers.
Toutefois, des thématiques sont évidentes pour assurer un niveau de compétences minimum, comme par exemple la configuration sécurisée des ressources de cloud computing depuis l'interface client.
Veuillez noter que nous ne donnons pas de précisions quant à la forme des formations ou l'organisme formateur : l'entité surveillée doit faire sa propre analyse et documenter son choix.

QUESTION 10 : Est-il nécessaire d'avoir un consentement d'un client pour stocker ses données sur une infrastructure de cloud computing sous-traitée ? (cf. point 25.a de la circulaire cloud computing)

Date de publication : 27 mars 2019

Comme pour toute sous-traitance, qu'elle tombe dans le champ de la circulaire CSSF 12/552, CSSF 17/656 ou CSSF 17/654, la responsabilité quant au secret professionnel incombe au professionnel du secteur financier (PSF) et c'est à lui de faire son analyse pour savoir s'il est nécessaire ou non d'avoir un consentement client, et sous quelle forme (explicite ou non).
Nous vous rappelons néanmoins que vous devez respecter l'article 41 de la loi du 5 avril 1993 (telle que modifiée) relative au secteur financier. A ce titre et en l'absence d'une jurisprudence sur la forme du consentement, il n'est pas exclu que certains clients puissent contester devant les tribunaux la validité de leurs consentements.

QUESTION 11 : Faut-il nécessairement remplir les 7 conditions décrites aux paragraphes 14 et 17 de la circulaire cloud computing pour qu'une sous-traitance soit qualifiée de « cloud computing » ?

Date de publication : 27 mars 2019

Oui, il est nécessaire que les 7 conditions décrites aux paragraphes 14 et 17 soient toutes respectées pour qu'une sous-traitance soit qualifiée de « cloud computing », au sens de la circulaire cloud computing.
Il est à noter que, pour évaluer le respect des conditions de certains produits, il est nécessaire pour l'entité surveillée de se documenter sur le fonctionnement des technologies utilisées et des processus opérés par le fournisseur de service de cloud computing. Notamment, en cas d'offre SaaS, l'élasticité des ressources (cf. point 14.d) peut ne pas être sous le contrôle de l'opérateur des ressources mais automatiquement gérée par le fournisseur des services de cloud computing, celui-ci ayant mis en place des mécanismes pour répartir la charge en fonction de l'utilisation. La condition « élasticité rapide » est donc transparente pour l'ESCR, mais bien appliquée par le fournisseur des services de cloud computing.

QUESTION 12 : Pour répondre au critère de « ressources partagées » (cf. point 14.c de la circulaire cloud computing), est-il nécessaire que le fournisseur de services de cloud computing utilise une technologie de virtualisation ?

Date de publication : 27 mars 2019

Non. Le fournisseur de services de cloud computing peut utiliser une technologie de virtualisation pour partager les ressources entre ses différents clients, mais ceci n'est pas une obligation. Par ailleurs, certaines solutions de cloud computing n'utilisent pas de technologie de virtualisation mais répondent bien aux 7 conditions (cf. paragraphes 14 et 17 de la circulaire cloud computing).

QUESTION 13 : La CSSF maintient-elle une liste de fournisseurs de services de cloud computing étrangers autorisés ?

Date de publication : 27 mars 2019

Les fournisseurs de services de cloud computing ne relèvent pas de la surveillance de la CSSF, sauf s'ils sont PSF de support en raison des activités qu'ils exercent. La CSSF n'autorise donc pas de fournisseurs de services de cloud computing étrangers. C'est à l'entité surveillée de s'assurer du respect de la circulaire cloud computing, notamment le respect des 7 critères (cf. paragraphes 14 et 17) et des exigences contractuelles (cf. paragraphe 31) par les fournisseurs de services de cloud computing étrangers.

QUESTION 14 : Mon entité surveillée fait partie d'un groupe international. La maison mère a signé un contrat avec un fournisseur de services de cloud computing et donne accès à l'infrastructure de cloud computing aux entités du groupe, dont mon entité surveillée. Dans cette configuration, la maison mère est signataire et mon entité surveillée est à la fois ESCR et opérateur des ressources. Or, la circulaire cloud computing ne permet pas que le signataire ne soit ni l'ESCR ni l'opérateur des ressources (cf. paragraphe 20). Que faire ?

Date de publication : 27 mars 2019

Afin que cette configuration puisse être en ligne avec les exigences du paragraphe 20, le contrat signé avec le fournisseur de services de cloud computing doit prévoir des droits identiques entre la maison mère et l'entité surveillée. Contractuellement, ceci peut prendre la forme des exemples suivants :

- le contrat avec le fournisseur de services de cloud computing mentionne l'entité surveillée (l'ESCR) comme « affiliée » et donne explicitement les mêmes droits entre le client (la maison mère) et ses affiliées ;
- le contrat avec le fournisseur de services de cloud computing laisse la possibilité à la maison mère de mandater l'entité surveillée pour exercer tous les droits explicités dans le contrat sur le fournisseur de services de cloud computing et un contrat entre la maison mère et l'entité surveillée prévoit la possibilité pour l'entité surveillée d'être mandatée à tout moment (cette demande doit pouvoir émaner de l'entité surveillée et de manière inconditionnelle).

Ainsi, le rôle de « signataire » au sens de la circulaire cloud computing est attribué à l'entité surveillée.