FINANCE & TECHNOLOGY LUXEMBOURG

REQUEST FOR INFORMATION
Luxembourg - 25 juin 2021

Table des matières

1. CONTENU ET OBJECTIFS

1.1. Présentation de l'association

Finance & Technology Luxembourg (FTL) est une association sans but lucratif de droit luxembourgeois. FTL a pour objectif d'informer, de sensibiliser sur tous les sujets en lien avec les PSF de support ainsi que favoriser l'échange et l'émulation entre les membres afin de contribuer activement au développement de l'écosystème des technologies financières au Luxembourg et au-delà.
Les changements induits par la transformation digitale avec l'intégration des technologies telles que le cloud, l'internet des objets, l'intelligence artificielle ou encore la blockchain ont rendu évidente la nécessité de rapprochement entre les PSF de support historiques et les FinTechs. FTL compte ainsi aujourd'hui plus de 50 membres PSF de support et FinTechs.
FTL agit en tant que représentant de ses membres auprès du gouvernement, de la CSSF, des institutions financières ainsi que des autres associations agissant pour le développement du secteur ICT et financier luxembourgeois.

1.2. Contexte et définition du besoin

L'agrément de PSF de support est un gage de qualité et de confiance envers les entités surveillées. Il est néanmoins difficilement commercialisable en l'état, étant une spécificité propre au Luxembourg. Il représente une charge administrative qui s'ajoute aux réglementations auxquelles les entités surveillées doivent se conformer. Il devient nécessaire de le réinventer afin de l'adapter à la situation actuelle de globalisation des marchés et des possibilités d'outsourcing offertes pour qu'il reste un atout pour les acteurs de la place luxembourgeoise.
Dans ce contexte, le Haut Comité de la place financière a mandaté FTL pour réaliser les travaux de modernisation du statut de PSF de support afin de recréer collégialement un contexte dynamisant pour les acteurs du secteur en fournissant un cadre innovant qui dégage de la valeur pour les clients et un avantage compétitif certain pour le Luxembourg.

De plus, dans son exercice de surveillance des entités surveillées, la CSSF demande des reportings très littéraires et textuels. Le contenu varie donc beaucoup d'une entité à une autre, ce qui ne facilite pas le travail de la CSSF (Il est demandé une vision des risques vis-à-vis du jugement que la direction en fait, laissant place à une certaine subjectivité), notamment pour réaliser sa mission de supervision transversale / de benchmark entre les entités.

En outre, un certain nombre de PSF de support sont certifiés sur des normes ISO, notamment pour leur système de management de la sécurité de l'information (ISO 27001). Cette procédure est également lourde d'un point de vue administratif. Les rapports et les contrôles effectués ne sont pas exploités dans le cadre de la surveillance effectuée par la CSSF, conduisant à une duplication des travaux réalisés.

Par ailleurs, une convergence entre l'agrément et la certification simplifierait le reporting vis-à-vis de la surveillance afin d'avoir une meilleure structuration et une lecture facilitée qui servirait à la fois à la CSSF dans son travail de supervision et aux clients et prospects des PSF de support.

Dans le cadre de son Groupe de Travail « Mapping du statut », FTL a réalisé un travail d'identification des normes et standards existants avec lesquels les exigences ICT et sécurité de la CSSF pourraient se rejoindre[1]. L'objectif n'est pas ici de « transformer » le statut en norme, l'agrément continuera d'exister, mais de fournir à la CSSF un standard sur lequel elle pourrait se baser dans son travail de surveillance des PSF de support. Les sociétés adhérant à la démarche pourraient ainsi fournir leur reporting sur base de cette norme / standard – sans devoir dupliquer le travail déjà réalisé pour celui-ci – tout en pouvant le fournir à leurs clients pour des besoins commerciaux ou d'outsourcing « oversight ».

Le Groupe de Travail a identifié le standard international ISAE 3000 comme étant celui qui offre le plus de points de convergence avec le statut de PSF de support (notamment compte tenu de la flexibilité de son périmètre qui permet de coller au plus près des exigences / besoins de la CSSF). De plus, le Groupe de Travail a pris connaissance d'une initiative de place similaire et réussie à Singapour. En effet, l'association des banques locales (ABS) y a établi des guidelines pour permettre aux sous-traitants « matériels » du secteur bancaire local de réaliser des rapports ISAE 3000 sur leur respect des exigences locales en matière de sous-traitance. Le document *"Guidelines on control objectives and procedures for outsourced service providers"* de l'ABS[2] définit le contenu d'un rapport d'audit de sous-traitant (« OSPAR »), à savoir les objectifs de contrôle et les activités de contrôle / procédures qui devraient être examinés par le Réviseur d'entreprises en charge du rapport.

L'objectif poursuivi par FTL est de proposer un livrable similaire à celui de l'ABS pour le marché local. Dans un premier temps, le livrable devrait porter sur les exigences définies dans la Circulaire CSSF 20/750 sur la gestion des risques ICT et sécurité ; cette circulaire ayant été publiée récemment et ses exigences étant perçues comme pérennes.

Compte tenu de la diversité des PSF de support et des services qu'ils proposent, il est entendu que la démarche de produire un rapport d'audit serait optionnelle. Par ailleurs, compte tenu des investissements préexistants de certains PSF de support en matière de certification ISO, il serait utile que le livrable intègre une annexe contenant un mapping entre l'Annexe A de la norme ISO 27001 et le périmètre du rapport d'audit.

Les livrables seront rédigés en anglais.

1.3. Portée / champ du RFI

Les objectifs du présent RFI sont :

- D'identifier les approches possibles pour définir les objectifs de contrôle et les activités de contrôle / procédures liés aux exigences définies dans la Circulaire CSSF 20/750 ;

[1] Exigences ICT considérées : Circulaire CSSF 11/504, Circulaire CSSF 17/654 telle que modifiée, Circulaire CSSF 17/656, Circulaire CSSF 20/750, RGPD et Article 41 de la Loi du 5 août 1993 sur le secteur financier ; normes et standards considérés : ISO 27001, ISO 27005 / 31000, ISO 33001, COBIT, ISO 22301, CMMI / ISO 15504, ISO 9001, ITIL/ ISO 20000, ISAE 3402 / SOC1, SOC2 et ISAE 3000

[2] https://www.abs.org.sg/industry-guidelines/outsourcing
https://www.abs.org.sg/docs/library/abs_outsource_guidelines.pdf

- D'identifier les approches possibles pour préparer un mapping entre l'Annexe A de la norme ISO 27001 et les objectifs de contrôle / activités de contrôle / procédures mentionnés ci-dessus ; et
- D'estimer les charges de travail associées aux deux activités ci-dessus.

Lors de l'analyse des réponses au RFI, FTL sélectionnera une « short list » de répondants à laquelle un RFP sera envoyé. Cet RFP arrêtera les approches et plannings attendus et aura pour objectif de réaliser la sélection finale de sociétés engagées pour rédiger le livrable.

2. PROCÉDURE

Cette partie présente la procédure à suivre pour soumettre les réponses au présent RFI.

2.1. Dates clés du RFI

Les dates ci-dessous sont prévues pour répondre au RFI.

Date limite de signification d'intention de répondre au RFI :	5 juillet 2021
Date limite pour introduire des questions :	9 juillet 2021
Date limite de réponse au RFI :	15 juillet 2021 à midi
Durée d'analyse des réponses :	30 août 2021
Décision sur la liste des présélectionnés pour les prochaines étapes :	20 septembre 2021

Note importante : les informations et dates données ci-dessus et les durées résultantes pour les activités correspondantes reflètent uniquement la situation actuelle du planning. FTL se réserve le droit de les ajuster au fur et à mesure en fonction de la situation et si requis. Dans ce cas, elles peuvent être modifiées à n'importe quel moment de la suite de la procédure.

2.2. Contacts FTL

Finance & Technology Luxembourg a.s.b.l.
B.P. 1304
L-1013 Luxembourg
RCS : F7436
celine.tarraube@fedil.lu

2.3. Questions pendant la durée du RFI

Les répondants sont invités à adresser toute demande relative au contenu du RFI et à la procédure à Céline Tarraube, secrétaire générale de FTL à l'adresse email : celine.tarraube@fedil.lu
Date limite pour les questions : 9 juillet 2021

2.4. Coûts engendrés par la réponse

Tous les coûts directs ou indirects liés à la préparation et la soumission de la réponse au RFI sont la seule responsabilité du répondant. Aucun coût ne peut et ne sera imputé à FTL, en totalité ou en partie, pour la réponse.

2.5. Acceptation des conditions

En soumettant une réponse au RFI, le répondant est supposé avoir agréé et accepté les conditions stipulées dans cet RFI.

3. INFORMATIONS À FOURNIR

Cette partie détaille toutes les informations requises de la part du répondant. Les informations fournies seront utilisées par FTL tel que stipulé dans le champ du RFI pour la finalité du projet défini. Les réponses au RFI devraient être conformes à la table des matières / indications ci-après. Les réponses au RFI peuvent être faites indifféremment en français ou en anglais.

3.1. Informations sur le répondant et capacités financières

Le répondant doit joindre une présentation de l'entreprise ou toute autre information jugée pertinente (max. 5 pages) dont notamment :

- Nom et contacts du répondant
- Adresse
- Chiffre d'affaires 2019 et 2020
- Nombre d'employés au Luxembourg, dont le nombre d'employés intervenant sur les sujets couverts par le RFI
- Exemples de missions passées pertinentes et réalisées au Luxembourg

3.2. Approche proposée

Le répondant doit joindre une présentation de l'approche que son entreprise propose pour répondre aux besoins suivants (max. 5 pages par besoin) :

- Besoin no. 1 – rédiger le livrable dont notamment la définition des objectifs de contrôle et les activités de contrôle / procédures liés aux exigences définies dans la Circulaire CSSF 20/750 – l'approche devrait détailler :
    - Une table des matières cible pour le livrable
    - Les critères techniques qui définissent (i) un objectif de contrôle valide et (ii) une activité de contrôle / procédure valides selon le standard ISAE 3000 (illustrés de quelques exemples)
    - La coordination avec le Groupe de Travail et le Conseil d'administration FTL (besoins et attentes éventuels, support(s), fréquence, etc.)

- Besoin no. 2 – rédiger l'annexe du livrable, à savoir le mapping entre l'Annexe A de la norme ISO 27001 et les objectifs de contrôle / activités de contrôle / procédures définis dans le cadre du besoin no. 1 ci-dessus – l'approche devrait détailler :
    - Structure cible du mapping
    - La coordination avec le Groupe de Travail et le Conseil d'administration FTL (besoins et attentes éventuels, support(s), fréquence, etc.)

N.B. : la réponse au RFI peut porter sur le besoin no. 1 et / ou le besoin no. 2.

3.3. Estimations de planning et de charge de travail

Le répondant doit joindre à sa réponse :

- Une estimation de planning de type « elapsed time » faisant apparaître les milestones et éventuelles dépendances (max. 1 page) ; et
- Une estimation de la charge de travail et le détail des hypothèses qui y sont associés (max. 1 page par besoin).

3.4. Equipe proposée

Le répondant doit joindre une présentation de l'équipe susceptible d'exécuter l'approche proposée :

- Présentation de la structure d'équipe type avec une description sommaire des différents rôles et de leurs responsabilités respectives (max. 1 page)
- CVs des membres possibles de l'équipe (max. 5 CVs)

1. GLOSSAIRE

Liste des abréviations contenues dans ce document :

ABS : The Association of Banks in Singapore
FTL : Finance & Technology Luxembourg
OSPAR : Outsourced Service Provider's Audit Report / rapport d'audit de sous-traitant
RFI : Request for information
RFP : Request for proposal