cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 22/828

Modification de la circulaire CSSF 20/750 relative aux exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité

Commission de Surveillance du Secteur Financier

Circulaire CSSF 22/828

Concerne : Modification de la circulaire CSSF 20/750 relative aux exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité

Luxembourg, le 29 décembre 2022

À tous les établissements de crédit et à tous les PSF

À tous les établissements de paiement et à tous les établissements de monnaie électronique

Mesdames, Messieurs,

L'objet de la présente circulaire est de modifier le paragraphe 4. « Exigence additionnelle pour les prestataires de services de paiement (PSP) » de la circulaire CSSF 20/750 afin d'introduire un formulaire en vue de la soumission d'une évaluation à jour et exhaustive des risques liés aux TIC et à la sécurité en relation avec les services de paiement prestés par les PSP (ci-après « PSP ICT Assessment ») et de fournir de plus amples informations sur l'objectif, le champ d'application ainsi que sur le processus et le délai de soumission de ce formulaire.

Le PSP ICT Assessment formulaire est à utiliser pour la première fois concernant l'année civile 2022 et à soumettre à la CSSF au plus tard le 31 mars 2023.

La version modifiée du paragraphe 4 est reprise avec « suivi des modifications » à l'annexe de la présente circulaire. La version révisée du paragraphe 4 entrera en vigueur à la date de publication de la présente circulaire.

La présente circulaire est applicable à partir de sa date de publication.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annexe 1 : Version modifiée du paragraphe 4 de la circulaire CSSF 20/750

Commission de Surveillance du Secteur Financier

Annexe 1 : Version modifiée du paragraphe 4 de la circulaire CSSF 20/750

4. Exigence additionnelle pour les prestataires de services de paiement (PSP)[1]

8. Ainsi qu'en dispose le paragraphe 24 de l'orientation « 1.3.5 Rapport à l'organe de direction »[2] et conformément à l'article 105-1(2) de la LSP, les PSP ont l'obligation de fournir à la CSSF une évaluation des risques à jour et exhaustive en matière de services de paiement (ci-après « PSP ICT Assessment »). ~~La forme et les délais sont les suivants :~~

   ~~a. pour les établissements de crédit, cette évaluation, signée par l'organe de direction, doit être présentée le plus tôt possible après la clôture de l'exercice et au plus tard le 30 avril de chaque année ;~~

   ~~b. pour les établissements de paiement et les établissements de monnaie électronique, cette évaluation doit faire l'objet d'une section dédiée au sein du rapport de la direction sur l'état du contrôle interne, qui doit être publié conformément aux exigences de la Circulaire CSSF 15/614, au plus tard le dernier jour du troisième mois après la date de clôture de l'exercice financier ; et~~

   ~~c. pour POST Luxembourg, cette évaluation devrait faire l'objet d'une section dédiée au sein du rapport de la direction sur l'état du contrôle interne, à publier conformément aux exigences de la circulaire CSSF 98/143, au plus tard un mois après l'assemblée générale annuelle approuvant les comptes annuels du PSP.~~

   La CSSF a développé un formulaire standardisé pour le PSP ICT Assessment à utiliser par tous les PSP.

   L'objectif de ce modèle standardisé du PSP ICT Assessment est de présenter des lignes directrices aux PSP quant aux attentes de la CSSF par rapport aux informations à fournir par le biais du PSP ICT Assessment, et ainsi atteindre un certain degré d'harmonisation et de comparabilité entre les différents PSP ICT Assessments.

[1] *Tels que définis à l'article 1(37) de la LSP.*

[2] *Paragraphe 24 de l'orientation « 3.3.5 Reporting » dans la version anglaise.*

En ce qui concerne le champ d'application du PSP ICT Assessment, il est à noter que :

- Les établissements dont le modèle d'affaires n'inclut pas la prestation de services de paiement (tels que définis à l'article 1 (38) de la LSP) n'ont pas à fournir de PSP ICT Assessment. À partir du moment où le modèle d'affaires d'un établissement inclut la prestation de services de paiement, l'établissement doit soumettre à la CSSF, pour l'année civile en question, un PSP ICT Assessment.
- Les succursales originaires d'un autre État membre de l'EEE établies au Luxembourg, qui offrent des services de paiement, n'ont pas à fournir de PSP ICT Assessment à la CSSF. Par contre, les PSP luxembourgeois qui ont établi des succursales dans d'autres pays de l'EEE, qui fournissent des services de paiement, doivent inclure ces succursales dans leur PSP ICT Assessment. Dans le cas de figure où l'évaluation des risques liés aux TIC et à la sécurité pour ces succursales s'écarte de celle du PSP, ceci est à préciser dans le PSP ICT Assessment[3].

Tous les PSP devront soumettre le formulaire « PSP ICT Assessment », dûment complété, à la CSSF sur une base annuelle, **au plus tard le 31 mars de chaque année et couvrant l'année civile précédente**.

Le modèle du PSP ICT Assessment est disponible sur le site Internet de la CSSF à l'adresse suivante :

https://edesk.apps.cssf.lu/

Le PSP ICT Assessment doit être validé par l'organe de direction du PSP, c'est-à-dire au moins par le membre de l'organe de direction responsable de la fonction TIC. Cette validation est à préciser dans la section y relative du PSP ICT Assessment.

Le PSP ICT Assessment, dûment complété et validé, doit être soumis sur une base annuelle par un membre de l'organe de direction à la CSSF exclusivement par le portail eDesk de la CSSF.

[3] *cf. Questions/Réponses de l'EBA, ID number 2018_4176*

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu