Commission de Surveillance
du Secteur Financier

Circulaire CSSF 25/882

sur les exigences relatives à l'utilisation de services TIC tiers pour les Entités financières soumises au règlement sur la résilience opérationnelle numérique (règlement DORA)

Circulaire CSSF 25/882

sur les exigences relatives à l'utilisation de services TIC tiers pour les Entités financières soumises au règlement sur la résilience opérationnelle numérique (règlement DORA)

À toutes les Entités financières définies à l'article 2, paragraphe 1, points a) à i), k) à m), p), r) et s), et au sens de l'article 2, paragraphe 2, du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (ci-après « règlement DORA »)[1].

Luxembourg, le 9 avril 2025

Mesdames, Messieurs,

À compter du 17 janvier 2025, les dispositions du règlement sur la résilience opérationnelle numérique (« règlement DORA ») (règlement (UE) 2022/2554) sont applicables aux Entités financières surveillées par la CSSF et relevant du champ d'application du règlement DORA.

L'objectif de cette circulaire est de leur fournir des instructions pratiques sur la soumission de certaines informations et rapports relatifs au recours aux prestataires tiers de services TIC et exigés par le règlement DORA.

Cette circulaire complète également le règlement DORA, notamment en rappelant certaines exigences générales concernant l'utilisation des services TIC[2] fournis par des tiers, en tenant compte notamment des lois nationales luxembourgeoises relatives aux services financiers.

[1] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011

[2] Services TIC tels que définis à l'article 3, point 21, du règlement DORA

TABLE DES MATIÈRES

Chapitre 1. Champ d'application et principes généraux

Sous-chapitre 1.1. Champ d'application

1. Les entités suivantes tombent dans le champ d'application de la présente circulaire :

   a) les établissements de crédit, les entreprises d'investissement, les opérateurs de marché exploitant une plate-forme de négociation et les dispositifs de publication agréés (APA) faisant l'objet d'une dérogation et les mécanismes de déclaration agréés (ARM) faisant l'objet d'une dérogation au sens de la loi du 5 avril 1993 relative au secteur financier (LSF) ;
   b) les établissements de paiement, les prestataires de services d'information sur les comptes et les établissements de monnaie électronique au sens de la loi du 10 novembre 2009 relative aux services de paiement (LSP) ;
   c) les prestataires de services sur crypto-actifs et les émetteurs de jetons se référant à un ou des actifs au sens du règlement (UE) 2023/1114 ;
   d) les dépositaires centraux de titres au sens de la loi du 6 juin 2018 relative aux dépositaires centraux de titres (Loi DCT) ;
   e) les contreparties centrales au sens de la loi du 15 mars 2016 relative aux produits dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux ;
   f) les sociétés de gestion de droit luxembourgeois relevant du chapitre 15 ou de l'article 125-2 du chapitre 16 et les succursales luxembourgeoises de gestionnaires de fonds d'investissement relevant du chapitre 17, et les sociétés d'investissement qui n'ont pas désigné de société de gestion au sens de l'article 27 de la loi du 17 décembre 2010 concernant les organismes de placement collectif ;
   g) les gestionnaires de fonds d'investissement alternatifs agréés au titre du chapitre 2 et les fonds d'investissement alternatifs gérés de manière interne au sens de l'article 4, paragraphe 1, point b), de la loi du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs (Loi GFIA) ;
   h) les institutions de retraite professionnelle agréées conformément à l'article 2, paragraphe 2, de la loi du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de société d'épargne-pension à capital variable (sepcav) et d'association d'épargne-pension (assep) ;
   i) les administrateurs d'indices de référence d'importance critique au sens de l'article 20, paragraphe 1, point b), du règlement (UE) 2016/1011 ;
   j) les prestataires de services de financement participatif au sens de la loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers.

2. Les dispositions de la présente circulaire s'appliquent à toutes les entités financières concernées, telles que définies au point 1a) à j) ci-dessus, ci-après dénommées collectivement « **Entités financières** » ou individuellement « **Entité financière** », y compris leurs succursales telles que prévues par les lois respectives.

3. Les succursales luxembourgeoises des Entités financières qui font partie d'une entité juridique dont le siège social est situé dans un autre État membre de l'Union européenne (succursales UE) sont exclues du champ d'application du 0 de la présente circulaire.

4. Les établissements de crédit importants dont la BCE est l'autorité compétente pour ce qui est de la surveillance prudentielle sont exclues du 0 de la présente circulaire.

Sous-chapitre 1.2. Recours à un tiers pour les services d'exploitation des TIC

5. Il est rappelé aux Entités financières qu'en ce qui concerne les accords relatifs à l'utilisation de services TIC fournis par des prestataires tiers de services TIC, elles doivent s'assurer que l'accès aux renseignements couverts par le secret professionnel est garanti conformément à l'article 41, paragraphe 2*bis* de la LSF ou à l'article 30, paragraphe 2*bis*, de la LSP, selon le cas.

6. Les accords contractuels avec un tiers situé au Luxembourg relatifs aux services TIC soumis à l'exigence d'un agrément conformément à l'article 29-3 de la LSF, à savoir les services de gestion/opération des TIC (y compris les services d'opération des ressources en cas d'utilisation de services en nuage[3]) fournis à certains types d'Entités financières[4], ne peuvent être conclus que si l'une des conditions suivantes est remplie :

   a. le prestataire de services est autorisé par la CSSF conformément à l'article 29-3 de la LSF de fournir de tels services ; ou

   b. le prestataire de services est par ailleurs autorisé à exercer ces activités, à savoir s'il s'agit d'un établissement de crédit, ou il s'agit d'une entité qui entre dans le champ d'application de l'article 1-1, paragraphe 2, point c), de la LSF qui fait partie du groupe auquel l'Entité financière appartient et qui traite exclusivement d'opérations de groupe.

7. Les Entités financières peuvent conclure des accords contractuels sur l'utilisation de services TIC autres que ceux visés au point 6 ci-dessus, avec tout prestataire de services TIC au Luxembourg ou à l'étranger. Ces accords d'externalisation doivent être établis dans le respect des exigences du point 5 ci-dessus. En particulier, si le prestataire de services n'est pas autorisé à accéder aux renseignements couverts par le secret professionnel conformément à l'article 41, paragraphe 2*bis*, de la LSF ou à l'article 30, paragraphe 2*bis*, de la LSP, selon le cas, le prestataire de services ne peut avoir accès à ces renseignements que s'il est supervisé, tout au long de sa mission, par une personne de l'Entité financière qui a la charge des TIC.

Sous-chapitre 1.3. Sauvegarde des positions comptables

8. Lorsqu'elle utilise un système comptable situé en dehors du Luxembourg (services d'hébergement de systèmes comptables) de manière indépendante ou dans le cadre de l'externalisation des tâches opérationnelles de la fonction comptable, l'Entité financière dispose, à la fin de chaque journée, d'une sauvegarde sécurisée de toutes les positions comptables de fin de journée, y compris les positions des clients, dans un format lisible, afin

[3] Il est renvoyé au chapitre 3 de la présente circulaire pour les définitions des services en nuage et de l'opération des ressources.

[4] Les différents types d'Entités financières sont énumérés à l'article 29, paragraphe 3 de la LSF.

de garantir une préparation autonome d'un bilan, d'un compte de profits et pertes et des positions des clients[5].

9. Cette sauvegarde doit être stockée dans les locaux de l'Entité financière au Luxembourg, d'une entité du groupe située dans l'EEE ou d'un autre prestataire de services (c'est-à-dire un prestataire de services différent de celui qui fournit le service d'hébergement du système comptable) situé dans l'EEE.

10. Les Entités financières agissant en qualité d'administrateur d'OPC au sens de la circulaire CSSF 22/811 doivent appliquer les exigences des points 8 et 9 ci-dessus en tenant compte du point 80 de la circulaire CSSF 22/811 qui contient des exigences similaires adaptées aux activités d'administration d'OPC.

Chapitre 2. Obligations de notification en vertu du règlement DORA

Sous-chapitre 2.1. Notification de projets d'accords contractuels portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes

11. Conformément à l'article 28, paragraphe 3, du règlement DORA, les Entités financières doivent informer en temps utile l'autorité compétente de tout projet d'accord contractuel portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes ainsi que lorsqu'une fonction est devenue critique ou importante.

12. Cette notification est effectuée en suivant les instructions et sur base des formulaires disponibles sur le site Internet de la CSSF.

13. Cette notification est à soumettre au moins trois (3) mois avant la prise d'effet de l'accord contractuel prévu. En cas de recours à un PSF de support luxembourgeois régi par les articles 29-3, 29-5 ou 29-6 de la LSF, ce délai de notification est réduit à un (1) mois. Tout projet d'accord contractuel qui n'a pas été notifié dans le délai de notification susmentionné et/ou pour lequel les instructions et, le cas échéant, les formulaires disponibles sur le site Internet de la CSSF n'ont pas été utilisés, sera considéré comme non notifié.

14. La notification est sans préjudice des mesures de surveillance ou de l'application de mesures contraignantes et/ou de sanctions administratives de l'autorité compétente dans le cadre de sa surveillance continue, lorsqu'il apparaît que ces projets ne se conforment pas au cadre légal et réglementaire applicable.

[5] L'objectif de cette exigence est de garantir qu'en cas d'interruption soudaine des services fournis par le prestataire de services, les dernières positions sont connues et disponibles pour l'Entité financière au Luxembourg ou dans l'EEE. L'objectif n'est pas d'assurer la continuité de la fonction comptable. La sauvegarde peut donc être une copie/image, par exemple par simple extraction à partir du système, des positions comptables, y compris des positions des clients.

15. Dans tous les cas, les Entités financières demeurent pleinement responsables de la conformité avec l'ensemble des lois et des réglementations pertinentes en ce qui concerne les projets d'accords contractuels sur l'utilisation des services TIC.

Sous-chapitre 2.2. Registre d'informations

16. Conformément à l'article 28, paragraphe 3, du règlement DORA, les Entités financières doivent tenir et mettre à jour, au niveau de l'entité et aux niveaux sous-consolidé et consolidé, un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers de services TIC.

17. Les Entités financières doivent soumettre leur registre à la CSSF annuellement au niveau individuel ou consolidé, le cas échéant[6], comme expliqué plus en détail sur le site Internet de la CSSF.

18. Le registre de l'année *n* doit contenir tous les accords conclus jusqu'à la fin de l'année n et doit être soumis entre le 28 février et le 31 mars de l'année *n+1* au plus tard, en suivant les instructions disponibles sur le site de la CSSF. Par voie de dérogation[7], pour la première année de collecte (2025), le registre doit contenir tous les accords conclus jusqu'au 31 mars 2025 et doit être soumis entre le 1er avril 2025 et le 15 avril 2025.

19. Après toute demande de la CSSF de corriger une donnée du registre, les Entités financières doivent effectuer la correction demandée sans délai et soumettre le registre corrigé à la CSSF.

20. En dehors de la période de soumission officielle définie au point 18 ci-dessus, la CSSF se réserve le droit de demander le registre d'informations à tout moment.

Chapitre 3. Utilisation de services d'informatique en nuage fournis par des prestataires tiers de services TIC

21. Ce chapitre fournit principalement des éclaircissements sur la définition de l'informatique en nuage (*cloud computing*) et des services en nuage en cas d'utilisation de services d'informatique en nuage fournis par des prestataires de services tiers, afin d'établir une identification et une distinction claires entre l'informatique en nuage et les services d'exploitation des ressources. En effet, comme indiqué au point 6 de la présente circulaire, au Luxembourg, les services relatifs aux opérations des ressources ne peuvent être fournis qu'à certains types d'Entités financières par des prestataires de services spécifiques.

[6] Conformément à l'article 3 de la décision conjointe des AES publiée le 8 novembre 2024 (*uniquement en anglais*)

[7] Conformément au communiqué de la CSSF publié le 15 janvier 2025 « Entrée en application du règlement DORA au 17 janvier 2025 ».

Sous-chapitre 3.1. Définitions relatives à l'informatique en nuage (*cloud computing*)

3.1.1. Terminologie spécifique

22. Pour l'application du présent chapitre, on entend par :

1) Services en nuage	les services fournis au moyen de l'informatique en nuage, à savoir un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (réseaux, serveurs, stockage, applications et services par exemple) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort ou d'intervention d'un prestataire de services. Les services sont considérés comme des services d'informatique en nuage au sens de la présente circulaire si les conditions définies à la section 3.1.2. sont remplies.
2) Interface client	la couche logicielle mise à disposition par le fournisseur de services d'informatique en nuage à l'Entité financière pour lui permettre de gérer ses ressources d'informatique en nuage.
3) Ressource d'informatique en nuage	toute capacité informatique (ex. serveur, stockage, réseau, etc.) mise à disposition par un fournisseur de services d'informatique en nuage.
4) Fournisseur de services d'informatique en nuage	toute entreprise proposant des services d'informatique en nuage correspondant à la définition figurant à la section 3.1.2.
5) Opération des ressources	le fait de gérer les ressources d'informatique en nuage mises à disposition via l'interface client. Par extension, on désigne par « opérateur des ressources » la personne physique ou morale qui utilise l'interface client pour gérer les ressources d'informatique en nuage.

3.1.2. Définition de l'informatique en nuage (*cloud computing*)

23. L'informatique en nuage est un modèle constitué des cinq caractéristiques essentielles suivantes[8]:

    a. Libre-service et à la demande : Une Entité financière[9] peut s'approvisionner en capacités informatiques (comme du temps serveur ou du stockage sur le réseau) selon ses besoins, de manière unilatérale et automatique, sans nécessité d'intervention humaine de la part du fournisseur de services d'informatique en nuage.

    b. Accès réseau étendu : Les capacités informatiques sont disponibles via le réseau et accessibles via des mécanismes standards qui favorisent l'utilisation par des plateformes hétérogènes, de types client-léger (par exemple, des navigateurs) ou client-lourd (par exemple, des applications spécifiques) sur des équipements variés (par exemple, téléphones portables, tablettes, ordinateurs portables et ordinateurs fixes).

    c. Ressources partagées : Les ressources informatiques du fournisseur de services d'informatique en nuage sont partagées afin de servir de multiples Entités (financières) dans un modèle « multi-tenant »[10]. Les ressources physiques et virtuelles sont dynamiquement allouées et réaffectées en fonction des demandes des Entités financières. L'Entité financière n'a, en règle générale, pas de contrôle ou pas la connaissance quant à l'emplacement exact des ressources mises à disposition. Elle peut néanmoins contrôler ou connaître l'emplacement à un niveau d'abstraction plus élevé (par exemple, le pays, la région ou le centre de données). Ces ressources informatiques partagées incluent, par exemple, le stockage, le traitement, la mémoire et la bande passante du réseau.

    d. Elasticité rapide : Les capacités informatiques peuvent être rapidement fournies et libérées, dans certains cas automatiquement, pour s'ajuster à la demande. Du point de vue de l'Entité financière, les capacités informatiques disponibles semblent souvent être illimitées et peuvent être livrées en n'importe quelle quantité et à tout moment.

    e. Service mesuré : Les systèmes d'informatique en nuage contrôlent et optimisent automatiquement l'utilisation des ressources en exploitant un indicateur de capacité à un niveau d'abstraction approprié au type de service (par exemple, stockage, traitement, bande passante et comptes d'utilisateurs actifs). L'utilisation des ressources peut être surveillée, contrôlée et rapportée au fournisseur et à l'Entité financière, assurant ainsi la transparence quant au service utilisé.

[8] La CSSF s'appuie sur les définitions proposées par des organisations internationales telles que le « National Institute of Standards and Technology » (NIST) ou l' Agence européenne chargée de la Sécurité des Réseaux et de l'Information (ENISA).

[9] Dans un souci de clarté, la définition prend le cas où l'Entité financière est elle-même opérateur des ressources utilisées.

[10] Une infrastructure matérielle ou logicielle permettant de servir plusieurs Entités (financières) via des ressources d'informatique en nuage partagées et à l'aide d'un modèle standardisé.

24. Les services sont considérés comme des services d'informatique en nuage au sens de la présente circulaire lorsque les cinq caractéristiques essentielles définies au point 23 sont réunies et que les deux exigences spécifiques suivantes sont remplies :

    a. Le personnel travaillant pour le fournisseur de services d'informatique en nuage ne peut en aucun cas accéder aux données et aux systèmes qu'une Entité financière détient sur l'infrastructure informatique en nuage sans avoir obtenu au préalable l'accord explicite de l'Entité financière et sans qu'un mécanisme de surveillance ne soit mis à la disposition de l'Entité financière pour contrôler ces accès. Ces accès doivent revêtir un caractère exceptionnel. Néanmoins, l'accès peut découler d'une obligation légale ou d'un cas d'extrême urgence suite à un incident critique touchant une partie ou l'ensemble des Entités (financières) du fournisseur de services d'informatique en nuage[11]. Tous les accès du fournisseur de services d'informatique en nuage doivent être restreints et encadrés par des mesures préventives et détectives en ligne avec les bonnes pratiques de sécurité et auditées au moins annuellement.

    b. La prestation de services d'informatique en nuage n'engendre aucune interaction manuelle de la part du fournisseur de services d'informatique en nuage pour la gestion quotidienne des ressources d'informatique en nuage utilisées par l'Entité financière[12] (par exemple, le provisionnement, la configuration ou la libération de ressources d'informatique en nuage). Ainsi, seul l'opérateur des ressources (qui est soit l'Entité financière, soit un tiers autre que le fournisseur de services d'informatique en nuage) gère son environnement TIC hébergé sur l'infrastructure d'informatique en nuage. Le fournisseur de services d'informatique en nuage peut néanmoins intervenir manuellement :

        i. pour la gestion globale des systèmes de TIC supportant l'infrastructure d'informatique en nuage (par exemple, maintenance du matériel physique, déploiement de nouvelles solutions non spécifiques à l'Entité financière) ; ou

        ii. dans le cadre d'une demande particulière de l'Entité financière (par exemple, pour provisionner une ressource d'informatique en nuage absente du catalogue proposé par le fournisseur ou insuffisante en performance).

Chapitre 3.2. Responsable de l'utilisation des services en nuage (*cloud officer*)

25. Par ailleurs, la CSSF rappelle aux Entités financières qu'elles doivent *garantir et maintenir des compétences adéquates au sein de l'Entité financière en matière de gestion et de sécurité du service utilisé* tel que précisé à l'article 11, paragraphe 2, point k), lettre c), des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC[13]. Elles

[11] En cas d'extrême urgence, il conviendra de prévenir les Entités financières a posteriori.

[12] C'est en effet un système automatisé qui permet de provisionner les ressources, d'où le point 24 a) spécifiant que le personnel ne peut accéder par défaut aux ressources de l'Entité financière.

[13] Règlement délégué (UE) 2024/1774 de la Commission du 13 mars 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC

doivent également garantir *une attribution claire des rôles et des responsabilités en matière de sécurité de l'information entre l'entité financière et le prestataire tiers de services TIC, conformément au principe selon lequel l'entité financière est pleinement responsable de son prestataire tiers de services TIC* tel que précisé à l'article 11, paragraphe 2, point k), lettre b), des mêmes normes techniques de réglementation.

26. Dans ce contexte, l'opérateur des ressources doit désigner parmi ses employés une personne, le « responsable de l'utilisation des services en nuage ».

    a. Le responsable de l'utilisation des services en nuage doit avoir pour responsabilité l'utilisation des services d'informatique en nuage et être garant des compétences du personnel gérant les ressources d'informatique en nuage. L'opérateur des ressources veillera à attribuer la fonction de responsable de l'utilisation des services en nuage à une personne qualifiée et maîtrisant les enjeux d'un accord TIC sur une infrastructure informatique en nuage. Le responsable de l'utilisation des services en nuage doit avoir des compétences suffisantes pour assumer sa fonction, sur la base d'une formation appropriée à la gestion et à la sécurité des ressources d'informatique en nuage, spécifique au fournisseur de services d'informatique en nuage. Cette fonction de responsable de l'utilisation des services en nuage peut être exercée par des personnes cumulant déjà d'autres fonctions au sein du département TIC ;

    b. Si l'opération des ressources est exercée par l'Entité financière, il est possible que le responsable de l'utilisation des services en nuage puisse cumuler pour responsabilité la gestion des relations avec le fournisseur de services d'informatique en nuage. Si l'Entité financière fait appel à un tiers pour l'opération des ressources d'informatique en nuage, elle devra connaître le nom du responsable de l'utilisation des services en nuage de l'opérateur des ressources.

Chapitre 4. Date d'application

27. La présente circulaire s'applique avec effet immédiat.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général