Commission de Surveillance
du Secteur Financier

Circulaire CSSF 22/806

telle que modifiée par la circulaire CSSF 25/883

Externalisation

Commission de Surveillance du Secteur Financier

En cas de divergence entre les textes français et anglais, le texte anglais prévaut.

Circulaire CSSF 22/806

telle que modifiée par la circulaire CSSF 25/883*

Concerne :Externalisation

Luxembourg, le 22 avril 2022

À tous les établissements de crédit et professionnels du secteur financier au sens de la loi du 5 avril 1993 relative au secteur financier (« LSF »)

À tous les établissements de paiement et établissements de monnaie électronique au sens de la loi du 10 novembre 2009 relative aux services de paiement (« LSP »)

À toutes les sociétés de gestion autorisées uniquement en vertu de l'article 125-1 du chapitre 16 de la loi du 17 décembre 2010 concernant les organismes de placement collectif (« Loi OPCVM »)

Mesdames, Messieurs,

Les entités surveillées qui tombent dans le champ d'application de la loi du 5 avril 1993 relative au secteur financier (**LSF**) et de la loi du 10 novembre 2009 relative aux services de paiement (**LSP**) sont tenues d'adopter un solide dispositif de gouvernance interne, qui doit comprendre une structure organisationnelle claire, des mécanismes adéquats de contrôle interne, y compris des procédures et pratiques administratives et comptables saines permettant et promouvant une gestion saine et efficace des risques, ainsi que des mécanismes de contrôle et de sécurité de leurs systèmes informatiques.

L'Autorité bancaire européenne (**EBA**) a publié des Orientations révisées relatives à l'externalisation (**EBA/GL/2019/02** ou les **Orientations**). La CSSF, en sa qualité d'autorité compétente, applique ces Orientations et les a ainsi intégrées dans sa pratique administrative et dans son approche réglementaire en vue de favoriser la convergence en matière de surveillance dans ce domaine au niveau européen.

Alors que les Orientations s'appliquent uniquement aux établissements de crédit, entreprises d'investissement et établissements de paiement et de monnaie électronique, la CSSF a choisi d'étendre le champ d'application de la présente circulaire afin de promouvoir la convergence au niveau national. Il est attendu de toutes les entités visées au point 2 qu'elles se conforment dûment à la présente circulaire et qu'elles prennent des mesures d'exécution proportionnelles à la nature, à la portée et à la complexité, y compris leurs risques, de leurs opérations.

La présente circulaire vient compléter le cadre régissant le dispositif de gouvernance interne en spécifiant des principes directeurs et en établissant des exigences détaillées additionnelles[1] que les entités surveillées sont tenues de respecter lorsqu'elles ont recours à l'externalisation. De ce fait, la présente circulaire doit être lue conjointement avec les dispositions légales pertinentes[2]

* Note du traducteur : certaines modifications qui ont été faites dans la version anglaise ne s'appliquent pas à la version française.

[1] De telles précisions sont marquées en italique dans les parties I et III de la circulaire.

[2] Les dispositifs d'externalisation doivent, à tout moment, être conformes aux exigences organisationnelles en matière d'externalisation conformément aux articles 36-2 ou 37-1, paragraphe 5, de la LSF et aux articles 11, paragraphe 4, ou 24-7, paragraphe 4, de la LSP, le cas échéant.

et les circulaires CSSF portant sur l'administration centrale, la gouvernance interne et la gestion des risques[3] telles qu'applicables aux entités surveillées.

La présente circulaire regroupe dans un seul document les exigences de surveillance régissant les dispositifs d'externalisation en matière de technologies de l'information et de la communication (TIC), qui, auparavant, étaient disséminées dans des circulaires individuelles.

La présente circulaire comprend trois parties: la première partie établit les exigences relatives aux dispositifs d'externalisation et inclut les définitions, le champ d'application, les principes généraux et les exigences applicables en matière de gouvernance ; la deuxième partie est dédiée aux exigences spécifiques relatives aux dispositifs d'externalisation en matière de TIC reposant ou non sur une infrastructure informatique en nuage (« infrastructure de cloud computing ») ; la troisième partie prévoit l'entrée en vigueur de la présente circulaire.

À compter du 17 janvier 2025, les dispositions du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique (**règlement DORA**) s'appliquent à toutes les entités financières telles que définies à l'article 2, paragraphe 1, points a) à t), du règlement DORA. De ce fait, la présente circulaire a été modifiée afin d'apporter de la clarté juridique au marché et d'éviter la duplication des exigences avec les dispositions prévues dans le règlement DORA. Cet alignement reflète l'engagement continu de la CSSF d'assurer la gestion efficace des risques liés aux prestataires tiers de services TIC au sein du secteur financier tout en tenant compte de l'évolution des cadres réglementaires européens.

[3] Par exemple, la circulaire CSSF 12/552 pour les établissements de crédit et la circulaire CSSF 20/758 pour les entreprises d'investissement.

Commission de Surveillance du Secteur Financier

TABLE DES MATIÈRES

Commission de Surveillance du Secteur Financier

Partie I - Dispositifs d'externalisation

Chapitre 1. Définitions, abréviations et acronymes

1. Sauf indication contraire, les termes utilisés et définis dans la LSF, dans la LSP et dans le règlement (UE) n° 575/2013 ont la même signification dans la présente circulaire. En outre, aux fins de la présente circulaire, on entend par :

Définitions :

1) Services en nuage (« cloud services »)	services fournis au moyen du cloud computing, 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 de cloud computing au sens de la présente circulaire si les conditions définies aux points 135 et 136 sont remplies.*
a. Cloud communautaire	infrastructure cloud accessible à une communauté d'Entités concernées précise, y compris à plusieurs Entités concernées d'un même groupe, en vue d'une utilisation exclusive.
b. Cloud hybride	infrastructure cloud composée d'au moins deux infrastructures cloud distinctes.
c. Cloud public	infrastructure cloud accessible au grand public en vue d'une utilisation ouverte.
d. Cloud privé	infrastructure cloud accessible à une seule Entité concernée en vue d'une utilisation exclusive.
2) Autorité compétente	*la CSSF ou la BCE comme autorité compétente pour la surveillance des entités conformément au point 2 de la présente circulaire.*
3) Activités fondamentales	*les activités des Entités concernées soumises à autorisation ou enregistrement par une autorité compétente.*

4) Fonction critique ou importante[4]	toute fonction considérée comme fonction critique ou importante, tel qu'énoncé aux points 18 à 20.
5) Fonction	tous processus, services ou activités.
6) Externalisation en matière de TIC	*accord, de quelque forme que ce soit, conclu entre une Entité concernée et un prestataire de services en vertu duquel ce prestataire de services prend en charge un processus de TIC ou exécute un service de TIC ou une activité de TIC qui autrement, serait exécuté par l'Entité concernée elle-même. Les services sont des services exclusivement relatifs aux TIC.*
7) Entité concernée	*toutes les entités surveillées conformément au point 2 de la présente circulaire.*
8) Fonctions de contrôle interne	*la fonction de gestion des risques, la fonction compliance et la fonction d'audit interne.*
9) Externalisation intragroupe[5]	*une externalisation par une Entité concernée à un prestataire de services qui appartient au même groupe.* *Pour les Entités concernées qui sont soumises à une surveillance sur une base consolidée conformément à leurs lois et règlements sectoraux ou qui appartiennent à un groupe soumis à une telle surveillance sur une base consolidée, il importe de noter que le champ d'application des dispositions régissant l'externalisation intragroupe s'étend au-delà du seul champ d'application d'une telle surveillance sur base consolidée.*
10) Titulaires de fonctions clés	*les personnes qui ont une influence notable sur la direction de l'Entité concernée mais qui ne*

[4] Dans le contexte de l'externalisation, le sens de « fonction critique ou importante » doit être lu conformément à la Loi MiFID et au règlement délégué (UE) 2017/565 complétant la directive MiFID II. À cet égard, les dispositifs d'externalisation comprennent ceux qui sont liés à des « fonctions critiques » en ce qui concerne le cadre pour le redressement et la résolution au sens de l'article 1, point 64, de la Loi BRRD.

[5] *Pour les établissements de crédit qui appartiennent à un réseau d'un organisme central ou font partie d'un système de protection institutionnel soumis aux conditions énoncées à l'article 113, paragraphe 7, du règlement CRR, une externalisation à un membre du réseau ou du système de protection institutionnel est considérée comme une externalisation intragroupe pour les besoins de la présente circulaire.*

	sont ni membres de l'organe de direction ni le directeur général. *Conformément aux dispositions spécifiques de la circulaire CSSF 12/552 et de la circulaire CSSF 20/758, ces personnes comprennent les responsables des fonctions de contrôle interne et peuvent inclure le responsable de la fonction financière (Chief Financial Officer, « CFO »), lorsqu'ils ne sont pas membres de l'organe de direction, et, lorsqu'ils sont identifiés selon une approche fondée sur les risques par les établissements, d'autres titulaires de fonctions clés.* *D'autres titulaires de fonctions clés pourraient inclure des responsables de lignes d'activité importantes, des succursales de l'Espace économique européen/l'Association européenne de libre-échange, des filiales de pays tiers et d'autres fonctions internes.*
11) Organe de direction	organe ou organes de l'Entité concernée, qui sont désignés conformément au droit national, qui sont compétents pour définir la stratégie, les objectifs et la direction globale de l'Entité concernée et qui assurent la supervision et le suivi des décisions prises en matière de gestion et, incluent, les personnes qui dirigent effectivement les activités de l'Entité concernée et les administrateurs et personnes responsables de la direction de l'Entité concernée. *Conformément aux circulaires CSSF pertinentes telles qu'applicables, le terme organe de direction comprend les notions de direction autorisée, conseil d'administration/ou conseil de gérance et/ou conseil de surveillance et conseil exécutif.*
12) État membre	*État membre de l'Union européenne. Par principe, ce terme inclut les pays de l'EEE autres que les pays de l'UE.*

13) a. Externalisation	accord, de quelque forme que ce soit, conclu entre une Entité concernée et un prestataire de services en vertu duquel ce prestataire de services prend en charge un processus ou exécute un service ou une activité qui autrement, serait exécuté par l'Entité concernée elle-même.
b. Sous-externalisation	situation dans laquelle le prestataire de services relevant d'un accord d'externalisation transfère lui-même à un autre fournisseur de services une fonction externalisée (« sous-traitant »). *Il peut y avoir des accords de sous-externalisation multiples dans un même accord d'externalisation.* La sous-externalisation *peut* aussi être désignée par « chaîne d'externalisation » ou « externalisation en chaîne ».
14) Prestataire de services	un tiers exécutant au titre d'un accord d'externalisation tout ou partie d'une procédure, d'un service ou d'une activité externalisé. *Dans ce contexte, une entité du groupe doit être considérée comme un tiers.*
15) Pays tiers	*un État autre qu'un État membre de l'Espace économique européen.*
Abréviations et acronymes :	
16) Loi LBC/FT	*loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme*
17) Loi BRRD	*loi modifiée du 18 décembre 2015 relative aux mesures de résolution, d'assainissement et de liquidation des établissements de crédit et de certaines entreprises d'investissement ainsi qu'aux systèmes de garantie des dépôts et d'indemnisation des investisseurs*
18) Établissement BRRD	*un établissement de crédit ou une entreprise d'investissement BRRD conformément à l'article 59-15, point (13), de la LSF*

19) règlement CRR	*règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement*
20) règlement DORA	*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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011*
21) EBA	*Autorité bancaire européenne*
22) BCE	*Banque centrale européenne*
23) EEE	*Espace économique européen*
24) ESMA	*Autorité européenne des marchés financiers*
25) RGPD	*règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données)*
26) TIC	*Technologies de l'information et de la communication*
27) LSF	*loi modifiée du 5 avril 1993 relative au secteur financier*
28) LSP	*loi modifiée du 10 novembre 2009 relative aux services de paiement*
29) directive MiFID II	*directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant les directives 2002/92/CE et 2011/61/UE*
30) Loi MiFID	*loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers*
31) Loi OPCVM	*loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif*

Chapitre 2. Champ d'application et proportionnalité

2. La présente circulaire définit les attentes en matière de surveillance à respecter lors d'un recours à l'externalisation.

La partie I de la présente circulaire est applicable aux Entités concernées suivantes lors de l'externalisation de services autres que des services TIC[6] :

- établissements de crédit[7] [8], y compris leurs succursales, au sens de la LSF ;

- entreprises d'investissement, y compris leurs succursales, au sens de la LSF ;

*- établissements de paiement et établissements de monnaie électronique, y compris leurs succursales, (dénommés chacun **établissement de paiement**) au sens de la LSP. Les prestataires de services d'information sur les comptes (**AISP**) fournissant uniquement le service visé au point 8 de l'annexe de la LSP ne sont pas inclus dans le champ d'application de la présente circulaire. Toute référence dans la présente circulaire aux « services de paiement » comprend les services de paiement ou l'émission de monnaie électronique fournis par les établissements de monnaie électronique ;*

La présente circulaire est pleinement applicable (partie I et partie II) aux Entités concernées suivantes :

*- professionnels du secteur financier spécialisés et de support (**PSF**), y compris leurs succursales, au sens de la LSF. Les succursales au Luxembourg de PSF ayant leur siège social dans un pays tiers sont réputées incluses dans la notion de PSF ;*

- POST Luxembourg régi par la loi du 15 décembre 2000 sur les services financiers postaux[9]. Toutes les dispositions applicables aux établissements de paiement le sont aussi à POST Luxembourg ;

- succursales au Luxembourg d'établissements de crédit, d'entreprises d'investissement et d'établissements de paiement ayant leur siège social dans un pays tiers. Elles sont réputées incluses dans la notion d'établissement de crédit, d'entreprise d'investissement et d'établissement de paiement.

[6] *Par souci de clarté, ces entités ne sont pas tenues d'inclure leurs dispositifs d'externalisation en matière de TIC dans le registre visé à la section 4.2.7.*
[7] *La BCE est l'autorité compétente pour la surveillance prudentielle des établissements de crédit importants (significant institutions - SI). Les SI doivent se référer aux règles de la BCE pertinentes (le cas échéant).*
[8] *La présente circulaire s'applique aux compagnies financières holding (mixtes) qui sont autorisées conformément à l'article 34-2 de la LSF. Voir aussi la circulaire CSSF 12/552, point 3 de la partie I.*
[9] *Par souci de clarté, le terme « services financiers postaux » est à comprendre au sens prévu à l'article 1 de la loi modifiée du 15 décembre 2000.*

La présente circulaire est aussi pleinement applicable aux entités suivantes établies au Luxembourg lorsqu'elles ont recours à l'externalisation en matière de TIC :

- sociétés de gestion autorisées uniquement en vertu de l'article 125-1 du chapitre 16 de la Loi OPCVM

Les Entités concernées doivent se conformer à la présente circulaire lors de la conception des dispositifs de gouvernance interne dans le contexte de leur modèle d'affaires dans son ensemble, en tenant, en particulier, dûment compte des activités réglementées par la LSF, la LSP ou toute autre loi nationale conférant compétence à la CSSF. En conséquence, la présente circulaire s'applique aussi lorsque les Entités concernées fournissent des services d'investissement et exécutent des activités d'investissement conformément à la Loi MiFID, conçoivent les dispositifs de gouvernance interne dans le contexte de la Loi LBC/FT ou fournissent des services de gestion d'actifs et des tâches de dépositaire pour les organismes de placement collectif établis au Luxembourg.

*Les succursales au Luxembourg des types d'entités susmentionnés qui font partie d'une entité légale dont le siège est situé dans un autre État membre de l'EEE (**succursales EEE**) sont soumises à la surveillance de l'autorité compétente de cet État membre (État membre d'origine). Cependant, étant donné que la CSSF est compétente pour s'assurer que les succursales EEE respectent les exigences spécifiques prévues dans les cadres réglementaires thématiques ou sectoraux[10], la partie I de la présente circulaire s'applique si des succursales EEE externalisent des fonctions qui relèvent de domaines pour lesquels la CSSF maintient une responsabilité de supervision, à l'exception de l'externalisation en matière de TIC[11]. Alors que la présente circulaire n'impose pas d'exigences spécifiques relatives aux dispositifs de gouvernance interne de succursales EEE, il convient tout de même que ces succursales adoptent des dispositifs de gouvernance interne comparables à ceux prévus par la présente circulaire, en coordination avec leur siège.*

3. Les dispositions de la présente circulaire s'appliquent à toutes les Entités concernées sur une base *individuelle*. Les établissements de crédit et les entreprises d'investissement doivent également se conformer à la présente circulaire sur une base sous-consolidée et consolidée, *compte tenu de leur périmètre prudentiel de consolidation*. Les établissements de crédit et entreprises d'investissement qui sont des entreprises mères doivent s'assurer

[10] *Notamment dans le contexte de services d'investissement conformément à la Loi MiFID, la Loi LBC/FT, la prestation de services de gestion d'actifs et l'exercice de tâches de dépositaire pour les organismes de placement collectif établis au Luxembourg.*

[11] *Ces dispositifs sont couverts par la circulaire CSSF 25/882 sur les exigences relatives à l'utilisation de services TIC tiers pour les entités financières soumises au règlement DORA et à la réglementation DORA.*

de la cohérence, de la bonne intégration et de l'*adéquation* des dispositifs, processus et mécanismes de gouvernance interne de leurs filiales, en vue de l'application effective de la présente circulaire à tous les niveaux pertinents de la *surveillance*[12].

4. Les Entités concernées doivent, lorsqu'elles se conforment à la présente circulaire, prendre en compte le principe de proportionnalité. *En vertu de ce principe, les Entités concernées doivent prendre des mesures d'exécution qui sont proportionnées à leur taille et à leur organisation interne de même qu'à la nature, à la portée et à la complexité de leurs activités ou services, y compris leurs risques. En tant que telles, les Entités concernées qui sont de grande taille, complexes ou s'engagent dans des activités ou services risqués doivent adopter un cadre plus solide pour leur administration centrale, leur gouvernance interne et leur gestion des risques. En revanche, les Entités concernées peuvent appliquer un cadre moins élaboré si leur taille et leur organisation interne, ainsi que la nature, la portée et la complexité de leurs activités et services, y compris leurs risques, le justifient.*

5. Ceci dit, les dispositifs d'externalisation peuvent avoir des répercussions sur le profil de risque des Entités concernées, notamment en ce qui concerne le risque opérationnel auquel elles peuvent être exposées (p. ex. risque de perturbations). En conséquence, les Entités concernées peuvent avoir besoin d'améliorer leurs cadre et procédures de contrôle interne afin d'intégrer cette dimension de risque modifiée dans leur cadre de gestion des risques à l'échelle de l'entité.

6. Afin de soutenir la mise en œuvre de la présente circulaire, les Entités concernées doivent documenter leur analyse de proportionnalité par écrit et faire approuver leurs conclusions par l'organe de direction.

Chapitre 3. Principes généraux régissant les dispositifs d'externalisation et l'externalisation intragroupe

Sous-chapitre 3.1 Principes généraux régissant les dispositifs d'externalisation

7. L'externalisation permet aux Entités concernées un accès relativement aisé à l'expertise y compris dans le domaine des nouvelles technologies et de réaliser des économies d'échelle, parvenant ainsi à améliorer leur rentabilité. Cependant, la mise en œuvre de dispositifs d'externalisation par les Entités

[12] Lorsqu'une exemption a été accordée conformément à l'article 10 du règlement CRR à des sociétés coopératives ou à l'article 7 du règlement CRR, les dispositions de la présente circulaire doivent être appliquées au niveau de l'entreprise mère, y compris pour ses filiales, ou par l'organe central et ses établissements affiliés dans leur ensemble.

concernées crée des risques spécifiques et doit être soumise à des exigences spécifiques conformément aux articles 36-2 et 37-1, paragraphe 5, de la LSF, et aux articles 11, paragraphe 4, et 24-7, paragraphe 4, de la LSP, le cas échéant.

Les dispositifs d'externalisation sont soumis aux principes suivants :

- Les dispositifs d'externalisation doivent être soumis à une supervision appropriée et ne peuvent, en aucun cas, aboutir à un contournement de l'esprit et de la lettre des exigences réglementaires ou des mesures prudentielles.

- Lors d'une externalisation de tâches opérationnelles à un prestataire de services, les Entités concernées doivent s'assurer que ces tâches opérationnelles sont effectivement exécutées. Les Entités concernées doivent effectuer un suivi et un audit appropriés des dispositifs d'externalisation, y compris via la réception de rapports conformément à la section 4.3.3 et la section 4.2.6 et la sous-section 4.3.2.3, respectivement.

- La responsabilité de l'organe de direction pour l'Entité concernée et toutes ses activités ne peuvent jamais être externalisées :

- *Aucune externalisation qui résulterait en une délégation par l'organe de direction de sa responsabilité, altérant la relation et les obligations des Entités concernées vis-à-vis de leurs clients, compromettant les conditions de leur autorisation ou supprimant ou modifiant une quelconque condition sur base de laquelle l'autorisation de l'Entité concernée a été accordée, n'est permise.*
- *L'Entité concernée demeure pleinement responsable de la mise en conformité avec les exigences réglementaires, y compris dans le cas d'une sous-externalisation, du fait qu'une sous-externalisation peut modifier le risque et la fiabilité des dispositifs d'externalisation. De ce fait, l'Entité concernée doit déterminer si la sous-externalisation est autorisée et adapter son cadre de gouvernance interne et de gestion des risques en ce qui concerne la sous-externalisation, et en particulier par rapport aux dispositifs d'externalisation critiques ou importants, alors que le prestataire de services initial est également soumis à des obligations de supervision.*

- Les dispositifs d'externalisation ne doivent pas créer des risques opérationnels indus. Les risques à prendre en compte comprennent ceux qui sont liés à la relation avec le prestataire de services, le risque causé pour avoir autorisé la sous-externalisation, le risque de concentration posé par des accords d'externalisation multiples au même prestataire de services et/ou le risque de concentration posé par l'externalisation de fonctions critiques ou importantes à un nombre limité de prestataires de services. Les Entités concernées doivent en tout état de cause gérer les risques de concentration et de dépendance de manière appropriée.

- L'externalisation ne doit pas nuire à la qualité et à l'indépendance des contrôles internes des Entités concernées ou à la capacité de ces entités à surveiller et superviser la conformité avec les exigences réglementaires et de poursuivre leurs activités en continuité d'exploitation (« going concern »).

- L'externalisation ne doit pas aboutir à une situation où les Entités concernées seraient en violation des obligations légales ou réglementaires en matière d'administration centrale et deviendraient des « coquilles vides » sans substance suffisante pour maintenir leur agrément. À cette fin, les organes de direction doivent s'assurer, y compris dans un contexte d'externalisation de fonctions à une entreprise mère ou à d'autres entités du groupe, que des ressources suffisantes sont disponibles afin de soutenir et d'assurer de manière appropriée l'exécution/exercice de leurs responsabilités, y compris la surveillance des risques et la gestion des dispositifs d'externalisation.

- Lors d'une externalisation, les Entités concernées doivent s'assurer que toutes les exigences de la présente circulaire sont respectées en permanence. Les fonctions considérées comme critiques d'un point de vue de la résolution peuvent également être externalisées à condition de ne pas créer d'obstacles à la résolvabilité de l'établissement BRRD.

8. Lorsqu'elles exécutent des contrats d'externalisation qui impliquent des informations soumises à des exigences de confidentialité, les Entités concernées doivent mettre en place des dispositifs de confidentialité appropriés et s'assurer de la conformité avec l'article 41, paragraphe 2bis, de la LSF ou l'article 30, paragraphe 2bis, de la LSP, le cas échéant.

9. Les Entités concernées doivent se conformer au RGPD et aux exigences de l'autorité luxembourgeoise compétente dans ce domaine, à savoir la Commission Nationale pour la Protection des Données (CNPD).

10. L'externalisation ne doit en aucun cas entraver l'exercice des pouvoirs de surveillance par les autorités compétentes concernant tous les aspects pertinents de la surveillance. Les dispositifs d'externalisation ne doivent, en particulier, pas avoir d'impact sur la capacité des autorités compétentes à surveiller et superviser la conformité des Entités concernées avec les exigences légales ou réglementaires en continuité d'exploitation ou la conformité des établissements BRRD du point de vue de la résolution.

Sous-chapitre 3.2 Externalisation intragroupe

11. *L'externalisation intragroupe n'est pas nécessairement moins risquée que l'externalisation à une entité extérieure au groupe. De ce fait, l'externalisation intragroupe est soumise au même cadre et aux mêmes conditions réglementaires que l'externalisation à des prestataires de services extérieurs au groupe. Lorsque des Entités concernées ont l'intention d'externaliser à des entités appartenant au même groupe, elles doivent également s'assurer que la*

raison pour laquelle elles sélectionnent une entité du groupe est objective. En particulier, l'entité du groupe doit être apte à exercer la fonction en question et le dispositif d'externalisation ne doit pas exposer les Entités concernées à un conflit d'intérêts indu.

12. *Lors d'une externalisation dans le même groupe, les Entités concernées peuvent avoir un degré de contrôle et d'informations plus élevé par rapport à la fonction externalisée et au prestataire de services, qu'elles pourraient prendre en compte dans leur évaluation des risques. Cependant, les Entités concernées ne doivent pas s'appuyer exclusivement sur leurs entités du groupe pour la gestion de l'externalisation et doivent concevoir des procédures de suivi et de supervision appropriés au niveau de l'Entité concernée elle-même afin d'être conformes avec les exigences énoncées dans la présente circulaire.*

13. *Sous réserve des principes généraux énoncés au sous-chapitre 3.1,* les Entités concernées qui ont recours à des dispositifs de gouvernance centralisés doivent *de ce fait* se conformer à ce qui suit :

a. lorsque les Entités concernées ont conclu des accords d'externalisation avec des prestataires de services au sein du groupe, l'organe de direction de l'Entité concernée conserve, pour ces accords d'externalisation également, l'entière responsabilité de veiller au respect de toutes les exigences réglementaires et de l'application effective de la présente circulaire ;

b. lorsque les Entités concernées ont des dispositifs d'externalisation avec un prestataire de services au sein du groupe, l'Entité concernée doit s'assurer que ces dispositifs d'externalisation, y compris les tâches opérationnelles externalisées, sont effectivement exécutées. Les Entités concernées doivent effectuer un suivi et un audit appropriés des dispositifs d'externalisation, y compris via la réception de rapports appropriés, conformément à la section 4.3.3 et à la section 4.2.6 et la sous-section 4.3.2.3, respectivement.

14. Outre le point 13 ci-dessus, les Entités concernées au sein d'un groupe doivent prendre en compte ce qui suit :

a. lorsque le suivi opérationnel de l'externalisation est centralisé (p. ex. dans le cadre d'un accord-cadre pour le suivi des dispositifs d'externalisation), les Entités concernées doivent veiller à ce qu'un suivi indépendant du prestataire de services et une surveillance appropriée par chaque Entité concernée soient possibles, y compris en recevant, au moins annuellement et sur demande, de la fonction de suivi centralisé, des rapports comprenant au moins un résumé de l'évaluation des risques et du suivi des performances *et en remettant en question ces rapports*. En outre, les Entités concernées doivent recevoir de la fonction de suivi centralisé un résumé des rapports d'audit pertinents *relatifs à l'externalisation* et, sur demande, le rapport d'audit complet.

L'organe de direction des Entités concernées doit déterminer si l'étendue et le contenu de ces rapports sont cohérents et appropriés et doivent prendre des mesures si ces rapports ne lui permettent pas d'être en conformité avec les exigences en matière de gouvernance interne et de gestion des risques telles que prévues dans d'autres circulaires CSSF ;

b. les Entités concernées doivent veiller à ce que leur organe de direction soit dûment informé des changements prévus pertinents concernant les prestataires de services qui font l'objet d'un suivi centralisé et de l'incidence potentielle de ces changements sur les fonctions critiques ou importantes assurées, y compris par l'intermédiaire d'un résumé de l'analyse des risques *comprenant* les risques juridiques, le respect des exigences réglementaires et l'incidence sur les niveaux de service, afin que les organes de direction puissent évaluer l'incidence de ces changements *et les accepter ou prendre des mesures appropriées* ;

c. lorsque les Entités concernées au sein du groupe s'appuient sur une évaluation centrale des dispositifs d'externalisation préalable à l'externalisation, chaque Entité concernée doit recevoir un résumé de cette évaluation et veiller à ce que, dans cette évaluation, sa structure et ses risques spécifiques soient pris en compte dans le processus décisionnel *et l'accepter ou prendre des mesures appropriées* ;

d. pour les Entités concernées au sein d'un groupe, le registre *tel que prévu à la section 4.2.7* peut être tenu de manière centralisée. Lorsque le registre de tous les dispositifs d'externalisation existants, est établi et tenu à jour de manière centralisée au sein d'un groupe, les autorités compétentes et toutes les Entités concernées doivent pouvoir obtenir le registre individuel sans délai indu. Ce registre doit inclure tous les accords d'externalisation, y compris les accords d'externalisation conclus avec des prestataires de services au sein de ce groupe. *Les Entités concernées doivent s'assurer que le registre est conforme aux dispositions de la section 4.2.7, relative aux exigences en matière de documentation ;*

e. *en ce qui concerne leurs stratégies de sortie*, pour une fonction critique ou importante, lorsque les Entités concernées s'appuient sur un plan de sortie qui a été établi au niveau du groupe, toutes les Entités concernées doivent recevoir un résumé du plan et s'assurer que celui-ci peut être effectivement exécuté, *conformément aux dispositions prévues à la section 4.3.4, relative aux Plans de sortie* ;

f. les Entités concernées faisant partie d'un groupe peuvent s'appuyer sur des plans de poursuite de l'activité établis de manière centralisée concernant leurs fonctions externalisées. Les Entités concernées doivent recevoir un résumé du plan *et s'assurer que le plan est conforme aux dispositions de la section 4.2.5, relative aux Plans de poursuite de l'activité.*

Chapitre 4. Gouvernance des dispositifs d'externalisation

Sous-chapitre 4.1 Évaluation des dispositifs d'externalisation

Section 4.1.1 Externalisation

15. Les Entités concernées doivent déterminer si un accord conclu avec un tiers relève de la définition de l'externalisation. Dans le cadre de cette évaluation, il convient d'examiner si la fonction (ou une partie de celle-ci) qui est externalisée vers un prestataire de services est exercée de manière récurrente ou continue par ce dernier et si cette fonction (ou une partie de celle-ci) relèverait normalement de fonctions qui seraient ou pourraient raisonnablement être exercées par des Entités concernées, même si l'Entité concernée n'a pas elle-même exercé cette fonction par le passé.

16. Lorsqu'un accord conclu avec un prestataire de services couvre plusieurs fonctions, les Entités concernées doivent tenir compte de tous les aspects de l'accord dans leur évaluation ; par exemple, si le service fourni comprend la fourniture de matériel de stockage de données et la sauvegarde des données, ces deux aspects doivent être examinés ensemble.

17. En règle générale, les Entités concernées ne doivent pas considérer les éléments suivants comme relevant de l'externalisation :

a. une fonction qui doit obligatoirement être exercée par un prestataire de services, p. ex. le contrôle légal des comptes ;
b. les services d'information de marché (p. ex. la fourniture de données par Bloomberg, Moody's, Standard & Poor's, Fitch) ;
c. les infrastructures de réseaux mondiaux (p. ex. Visa, MasterCard) ;
d. les mécanismes de compensation et de règlement entre les chambres de compensation, les contreparties centrales et les établissements de règlement et leurs membres ;
e. les infrastructures de messagerie financière mondiale qui sont soumises à la surveillance d'autorités pertinentes ;
f. les services de correspondance bancaire ; et
g. l'acquisition de services qui, autrement, ne seraient pas assurés par l'Entité concernée (p. ex. conseils d'un architecte, *conseils* juridiques et représentation devant les tribunaux et les organes administratifs, nettoyage, jardinage et entretien des locaux de l'Entité concernée, services médicaux, entretien des voitures de fonction, restauration, services de distributeurs automatiques, services de bureau, services de voyage, services de gestion du courrier, accueil, secrétariat et standardistes), de

biens (p. ex. cartes plastiques[13], lecteurs de cartes, fournitures de bureau, ordinateurs personnels, meubles) ou les services d'équipement (p. ex. électricité, gaz, eau, ligne téléphonique).

Section 4.1.2 Fonctions critiques ou importantes

18. Les Entités concernées doivent toujours considérer une fonction comme critique ou importante dans les situations suivantes :

a. lorsqu'une anomalie ou une défaillance de son exécution est susceptible de nuire sérieusement :

   i. à la capacité des Entités concernées de se conformer de manière continue aux conditions de leur agrément et/ou à leurs autres obligations *légales* et réglementaires ;

   ii. à leurs performances financières ; ou

   iii. à la solidité ou à la continuité de leurs services et activités ;

b. lorsque les tâches opérationnelles des fonctions de contrôle interne *ou des tâches opérationnelles de la fonction financière et comptable telle que prévues aux points 21 à 29* sont externalisées ;

c. lorsque *les établissements de crédit et les établissements de paiement* ont l'intention d'externaliser des fonctions d'activités bancaires ou de services de paiement dans une mesure qui nécessiterait l'autorisation[14] de l'autorité compétente *pertinente telle que prévue aux points 61 à 63*.

19. Dans le cas des établissements *BRRD*, une attention particulière doit être accordée à l'évaluation du caractère critique ou de l'importance des fonctions si l'externalisation concerne des fonctions liées à des activités fondamentales et des fonctions critiques *conformément à la Loi BRRD*[15] et identifiées par ces établissements selon les critères énoncés aux articles 6 et 7 du règlement délégué (UE) 2016/778 de la Commission[16]. Les fonctions nécessaires à

[13] *Ne couvre pas l'émission d'instruments de paiement telle que l'émission de cartes de crédit, qui est un service de paiement régulé relevant de la LSP.*
[14] Cf. les activités énumérées à l'annexe I de la LSF et à l'annexe de la LSP relative aux services de paiement.
[15] *« Fonctions critiques » en vertu de l'article 1, point 64, de la Loi BRRD désigne les activités, services ou opérations dont l'interruption est susceptible, dans un ou plusieurs États membres, d'entraîner des perturbations des services indispensables à l'économie réelle ou de perturber la stabilité financière en raison de la taille ou de la part de marché de l'établissement BRRD ou du groupe, de son interdépendance interne et externe, de sa complexité ou des activités transfrontalières qu'il exerce, une attention particulière étant accordée à la substituabilité de ces activités, services ou opérations.*
[16] Règlement délégué (UE) n° 2016/778 de la Commission du 2 février 2016 complétant la directive 2014/59/UE du Parlement européen et du Conseil en ce qui concerne les circonstances et les conditions dans lesquelles le paiement de contributions ex post extraordinaires peut être partiellement ou totalement reporté, et en ce qui concerne les critères de détermination des activités, services et opérations constitutifs de fonctions critiques et les critères de détermination des activités et services associés constitutifs d'activités fondamentales.

l'exécution d'activités fondamentales ou de fonctions critiques doivent être considérées comme des fonctions critiques ou importantes aux fins de la présente circulaire, à moins que l'évaluation de l'établissement *BRRD* n'établisse que le non-exercice de la fonction externalisée ou l'exercice inapproprié de la fonction externalisée n'aurait pas d'incidence négative sur la continuité opérationnelle de l'activité fondamentale ou de la fonction critique.

20. Lorsqu'elles évaluent si un dispositif d'externalisation se rapporte à une fonction critique ou importante, les Entités concernées doivent tenir compte, outre des résultats de l'évaluation des risques énoncée aux *points 66 à 70*, au moins des facteurs suivants :

a. si le dispositif d'externalisation est directement lié à la *fourniture d'activités fondamentales essentielles* ;

b. l'incidence potentielle de toute perturbation de la fonction externalisée ou de l'incapacité du prestataire de services à assurer le service aux niveaux de service convenus, de manière continue, en prenant en compte les éléments suivants :

i. leur résilience et leur viabilité financière à court et à long terme, y compris, le cas échéant, leurs actifs, capital, coûts, financement, liquidités, profits et pertes ;

ii. la poursuite de l'activité et la résilience opérationnelle ;

iii. les risques opérationnels, y compris les risques liés à la conduite, aux TIC et les risques juridiques ;

iv. les risques de réputation ;

v. le cas échéant, la planification du redressement et de la résolution, la résolvabilité et la continuité opérationnelle dans une situation d'intervention précoce, de redressement ou de résolution ;

c. l'incidence potentielle du dispositif d'externalisation sur leur capacité :

i. à identifier, et gérer tous les risques ;

ii. à se conformer à toutes les exigences légales et réglementaires ;

iii. à effectuer les audits appropriés concernant la fonction externalisée ;

d. l'incidence potentielle sur les services fournis à leurs clients ;

e. tous les dispositifs d'externalisation, l'exposition globale de l'Entité concernée à un même prestataire de services et l'incidence cumulative potentielle des dispositifs d'externalisation dans un même domaine d'activité ;

f. la taille et la complexité de tout domaine d'activité touché ;

g. la possibilité que le dispositif d'externalisation proposé puisse être étendu sans remplacer ou réviser l'accord sous-jacent ;

h. la capacité de transférer le dispositif d'externalisation proposé vers un autre prestataire de services, si nécessaire ou souhaitable, tant sur le plan contractuel que dans la pratique, y compris les risques estimés, les obstacles à la poursuite de l'activité, les coûts et le délai nécessaire pour procéder au transfert (« substituabilité ») ;

i. la capacité de réinternaliser la fonction externalisée dans l'Entité concernée, si nécessaire ou souhaitable ;

j. la protection des données et l'impact potentiel d'une violation de la confidentialité ou d'un manquement à l'obligation de garantir la disponibilité et l'intégrité des données sur l'Entité concernée et ses clients, notamment, mais non exclusivement, le respect du RGPD.

Section 4.1.3 Dispositifs d'externalisation relatifs aux fonctions de contrôle interne

21. Les dispositifs d'externalisation des fonctions de contrôle interne ne doivent pas avoir pour conséquence effective un transfert de ces fonctions dans leur ensemble au(x) prestataire(s) de services. De ce fait, les dispositifs d'externalisation doivent être limités, en principe, aux tâches opérationnelles de ces fonctions.

22. Les dispositifs d'externalisation de tâches opérationnelles des fonctions de contrôle interne ne doivent pas compromettre la permanence des dispositifs et des fonctions de contrôle interne de l'Entité concernée ou leur efficacité permanente. En pratique, cela signifie que les dispositifs d'externalisation doivent être proportionnés et ne doivent pas aboutir à vider les fonctions de contrôle interne des Entités concernées de leur substance.

23. Conformément aux exigences de la section 4.3.1.2, les Entités concernées doivent s'assurer que le prestataire de services remplit les exigences d'adéquation applicables et qu'il dispose de connaissances et d'une expérience techniques appropriées et suffisantes. En particulier, le prestataire de services doit faire preuve de connaissances appropriées et à jour du cadre réglementaire qui s'applique à l'Entité concernée.

24. Lors de l'externalisation de tâches opérationnelles des fonctions de contrôle interne, le prestataire de services doit être soumis à la surveillance de la personne responsable de la fonction de contrôle interne pertinente de l'Entité concernée (p. ex. le Chief Compliance Officer, le Chief Risk Officer ou le Chief Internal Auditor) et lui rapporter directement. Lorsque les Entités concernées externalisent l'ensemble des tâches opérationnelles de leur fonction de contrôle interne, le prestataire de services doit rapporter au membre de l'organe de direction responsable de la fonction de contrôle interne.

25. Dans le contexte de la fonction d'audit interne, le prestataire de services doit également avoir un accès direct à l'organe de direction dans l'exercice de

sa fonction de surveillance ou, le cas échéant, au président du comité d'audit. En outre, le prestataire de services doit réaliser les tâches opérationnelles d'audit interne conformément au plan d'audit interne et au plan de travail de l'Entité concernée, documenter le travail et les résultats de chaque mission de façon suffisamment détaillée et émettre un rapport dédié relatif à chaque mission. Tous les documents doivent être rédigés en français, allemand ou anglais et remis à la personne responsable de la fonction d'audit interne, à l'organe de direction et, le cas échéant, au comité d'audit.

Section 4.1.4 Dispositifs d'externalisation relatifs à la fonction financière et comptable

26. Les dispositifs d'externalisation de la fonction financière et comptable ne doivent pas avoir pour conséquence effective un transfert de cette fonction dans son ensemble au(x) prestataire(s) de services. De ce fait, les dispositifs d'externalisation doivent être limités, en principe, aux tâches opérationnelles de cette fonction. Les dispositifs d'externalisation de tâches opérationnelles des fonctions financière et comptable ne doivent pas compromettre la permanence de l'administration centrale de l'Entité concernée.

27. Lors de l'externalisation de tâches opérationnelles de la fonction comptable, les Entités concernées doivent disposer, à la fin de chaque jour, d'un accès inconditionnel et sans restriction à la balance de tous les comptes et de tous les mouvements comptables de la journée, afin de pouvoir fournir ces informations à l'autorité compétente ou tout autre organe, tel que requis par les lois et règlements applicables.

28. Lorsqu'elles utilisent un système comptable situé en dehors du Luxembourg (externalisation de l'hébergement du système comptable) indépendamment ou en relation avec l'externalisation de tâches opérationnelles de la fonction comptable, les Entités concernées doivent disposer, à la fin de chaque jour, de sauvegardes sécurisées de toutes les positions comptables de fin de journée, y compris les positions client, dans un format lisible, afin de garantir l'établissement autonome d'un bilan, d'un compte de profits et pertes et de positions client.

Cette sauvegarde doit être stockée soit dans les locaux de l'Entité concernée dans l'EEE, soit dans les locaux d'une entité du groupe située dans l'EEE, ou encore dans les locaux d'un autre prestataire de services (c'est-à-dire un prestataire de services différent de celui auprès duquel le système comptable est externalisé) situé dans l'EEE. Le système comptable doit permettre de tenir des comptes réguliers conformément au référentiel comptable applicable au Luxembourg, d'établir les comptes statutaires et d'établir les rapports prudentiels à l'intention de l'autorité compétente.

29. Dans le cas d'une externalisation de la production de rapports prudentiels, la personne responsable de la fonction financière et comptable au sein de l'Entité

concernée doit s'assurer que ces rapports représentent fidèlement la situation prudentielle de l'Entité concernée et qu'ils sont établis conformément aux instructions applicables. En outre, cette personne doit être en mesure d'assurer que les comptes annuels de l'Entité concernée sont établis conformément aux lois et règlements comptables applicables[17].

Sous-chapitre 4.2 Cadre de gouvernance

Section 4.2.1 Dispositifs de bonne gouvernance et risque de tiers

30. Dans le cadre du dispositif de contrôle interne d'ensemble, y compris les mécanismes de contrôle interne[18], les Entités concernées doivent disposer d'un cadre global de gestion des risques à l'échelle de l'entité, s'étendant à toutes les activités et unités internes. Dans ce cadre, les Entités concernées doivent identifier et gérer tous les risques auxquels elles sont exposées, y compris les risques résultant d'arrangements avec des tiers. Le cadre de la gestion des risques doit également permettre aux Entités concernées de prendre des décisions éclairées en matière de prise de risques et de veiller à ce que les mesures de gestion des risques soient mises en œuvre de façon appropriée, notamment en ce qui concerne les cyber-risques[19].

31. Les Entités concernées, compte tenu du principe de proportionnalité, doivent identifier, évaluer, surveiller et gérer tous les risques auxquels elles sont ou pourraient être exposés dans le cadre d'arrangements conclus avec des tiers, qu'il s'agisse ou non d'accords d'externalisation. Les risques, en particulier les risques opérationnels, de tous les arrangements conclus avec des tiers, doivent être évalués conformément aux points 66 à 70.

32. Les Entités concernées doivent veiller à se conformer à toutes les exigences du *RGPD*, y compris en ce qui concerne les arrangements conclus avec des tiers et les accords d'externalisation.

Section 4.2.2 Dispositifs de gouvernance sains pour l'externalisation

33. L'externalisation de fonctions ne doit entraîner aucune délégation des responsabilités de l'organe de direction. L'*organe de direction* demeure entièrement responsable du respect de toutes ses obligations réglementaires *ou*

[17] *La loi du 17 juin 1992 relative aux comptes annuels et comptes consolidés des établissements de crédit soumis aux lois luxembourgeoises pour les établissements de crédit ou la loi modifiée du 19 décembre 2002 concernant le registre de commerce, les règles comptables et les comptes annuels de sociétés pour les autres Entités concernées.*
[18] *Voir également les articles 6, 7, 24-2 et 24-3 de la LSP, le cas échéant.*
[19] *Voir également la circulaire CSSF 20/750 relative à la gestion des risques liés aux TIC et à la sécurité.*

ses responsabilités envers ses clients, y compris sa capacité à surveiller l'externalisation de fonctions critiques ou importantes.

34. L'organe de direction conserve en permanence l'entière responsabilité pour au moins :

a. s'assurer que l'Entité concernée satisfait en permanence aux conditions qu'elle doit remplir pour rester agréée, y compris aux conditions imposées par l'autorité compétente, le cas échéant ;

b. l'organisation interne de l'Entité concernée ;

c. l'identification, l'évaluation et la gestion des conflits d'intérêts ;

d. la définition des stratégies et politiques de l'Entité concernée (p. ex. le modèle d'entreprise, l'appétit pour le risque, le cadre de la gestion des risques) ;

e. la surveillance de la gestion quotidienne de l'Entité concernée, y compris la gestion de tous les risques associés à l'externalisation ; et

f. le rôle de contrôle de l'organe de direction dans sa fonction de surveillance, y compris de supervision et de contrôle du processus décisionnel de la direction.

35. L'externalisation ne doit pas abaisser les exigences en matière d'adéquation d'aptitudes applicables aux membres de l'organe de direction et aux titulaires de fonctions clés d'une Entité concernée. Les Entités concernées doivent disposer de compétences adéquates et de ressources suffisantes et disposant des qualifications appropriées pour assurer une gestion et un contrôle appropriés des dispositifs d'externalisation.

36. Les Entités concernées doivent :

a. attribuer clairement les responsabilités en matière de documentation, de gestion et de contrôle des dispositifs d'externalisation ;

b. allouer des ressources *qualifiées* suffisantes pour garantir le respect *des* exigences légales et réglementaires, y compris de *la présente circulaire* ainsi que de la documentation et du suivi de tous les dispositifs d'externalisation ;

c. *pour chaque activité externalisée, désigner parmi ses employés une personne qui aura la responsabilité de la gestion de la(des) relation(s) d'externalisation ainsi que de la gestion des accès aux données confidentielles ; et*

d. établir une fonction d'externalisation ou désigner un cadre *suffisamment* supérieur rendant compte directement à l'organe de direction (p. ex. un responsable d'une fonction de contrôle clé) et chargé de gérer et de contrôler les risques liés aux dispositifs d'externalisation conformément au

cadre de contrôle interne des Entités concernées, ainsi que de superviser la documentation des dispositifs d'externalisation. Les *entités de petite taille*[20] doivent au moins assurer une répartition claire *et saine* des tâches et des responsabilités en matière de gestion et de contrôle des dispositifs d'externalisation, et peuvent confier la fonction d'externalisation à un membre de l'organe de direction de l'Entité concernée.

37. Les Entités concernées doivent conserver en permanence une structure suffisante et ne pas devenir des « coquilles vides » ou des « sociétés boîtes aux lettres ». À cette fin, elles doivent :

a. satisfaire en permanence à toutes les conditions de leur agrément, y compris l'exercice effectif par l'organe de direction de ses responsabilités telles que définies au point 34 ;

b. conserver un cadre et une structure organisationnels clairs et transparents qui leur permettent d'assurer le respect des exigences légales et réglementaires ;

c. exercer un contrôle approprié et être en mesure de gérer les risques engendrés par l'externalisation de fonctions critiques ou importantes, *en particulier lorsque* les tâches opérationnelles des fonctions de contrôle interne, *de la fonction financière et comptable ou des activités fondamentales* sont externalisées ; et

d. disposer de ressources *qualifiées* et de capacités suffisantes pour assurer le respect des points a. à c. ci-dessus.

38. Lors de *la mise en place* d'un *dispositif* d'externalisation, les Entités concernées doivent au moins veiller :

a. à ce qu'elles puissent prendre et mettre en œuvre les décisions relatives à leurs activités commerciales et à leurs fonctions critiques ou importantes, y compris celles qui ont été externalisées ;

b. à maintenir la régularité de leurs activités et, *pour les établissements de crédit et établissements de paiement*, dans le cadre des services bancaires et des services de paiement qu'ils fournissent ;

c. à ce que les risques liés aux dispositifs d'externalisation actuels et prévus soient adéquatement identifiés, évalués, gérés et atténués, y compris les risques liés aux TIC et à la technologie financière (fintech) ;

[20] *Les établissements de crédit et les entreprises d'investissement doivent se référer aux circulaires CSSF 12/552 et CSSF 20/758 pour l'évaluation des entités de petite taille.*

d. à ce que des dispositifs de confidentialité appropriés soient mis en place en ce qui concerne les données et autres informations ;

e. à ce que l'information puisse circuler avec les prestataires de services ;

f. en ce qui concerne l'externalisation de fonctions critiques ou importantes, à être en mesure d'entreprendre au moins l'une des actions suivantes dans un délai approprié :

   i. transférer la fonction vers d'autres prestataires de services ;

   ii. réinternaliser la fonction ; ou

   iii. interrompre les activités commerciales qui dépendent de la fonction.

g. lorsque des données à caractère personnel sont traitées par des prestataires de services situés dans *l'EEE* et/ou dans des pays tiers, à ce que des mesures appropriées soient mises en œuvre et à ce que les données soient traitées conformément au *RGPD* ;

h. à ce que des dispositifs appropriés de confidentialité soient mis en place et s'assurer de la conformité avec l'article 41, paragraphe 2bis, de la LSF ou l'article 30, paragraphe 2bis, de la LSP, le cas échéant.

Section 4.2.3 Politique d'externalisation

39. L'organe de direction d'une Entité concernée qui a mis en place des dispositifs d'externalisation ou qui envisage de mettre en œuvre de tels dispositifs doit approuver, examiner régulièrement et mettre à jour une politique d'externalisation écrite et veiller à son application, le cas échéant, sur une base individuelle, sous-consolidée et consolidée. Pour les établissements de crédit et les entreprises d'investissement, la politique d'externalisation doit notamment prendre en compte les exigences *relatives à la « Procédure d'approbation de nouveaux produits » (« New Product Approval Process »)*[21].

40. La politique doit inclure les principales phases du cycle de vie des dispositifs d'externalisation et définir les principes, les responsabilités et les processus liés à l'externalisation. Plus particulièrement, la politique doit couvrir au moins :

a. les responsabilités de l'organe de direction conformément aux points 33 et 34, y compris sa participation, le cas échéant, à la prise de décisions concernant l'externalisation de fonctions critiques ou importantes ;

[21] *Veuillez vous référer à la partie II, sous-chapitre 7.3 de la circulaire CSSF 12/552 pour les établissements de crédit ou à la partie II, sous-chapitre 7.3 de la circulaire CSSF 20/758 pour les entreprises d'investissement.*

b. la participation des activités, des fonctions de contrôle interne et d'autres personnes dans les dispositifs d'externalisation ;

c. la planification des dispositifs d'externalisation, et notamment :

   i. la définition des exigences commerciales relatives aux dispositifs d'externalisation ;

   ii. les critères, y compris ceux mentionnés aux points 18 à 20, et les processus d'identification des fonctions critiques ou importantes ;

   iii. l'identification, l'évaluation et la gestion des risques conformément aux points 66 à 70 ;

   iv. les vérifications nécessaires à l'égard des prestataires de services potentiels, y compris les mesures exigées en vertu des points 71 à 75 ;

   v. les procédures d'identification, d'évaluation, de gestion et d'atténuation des conflits d'intérêts potentiels, conformément aux points 43 à 46 ;

   vi. la planification de la poursuite de l'activité conformément aux points 47 à 50 ;

   vii. le processus d'approbation des nouveaux dispositifs d'externalisation. *Ce processus doit prendre en compte l'exigence de délai additionnel en raison de la notification préalable à l'autorité compétente conformément aux points 59 et 60 ;*

d. la mise en œuvre, le suivi et la gestion des dispositifs d'externalisation, y compris :

   i. l'évaluation continue des performances du prestataire de services conformément aux points 104 à 110 ;

   ii. les procédures de notification et de réaction aux changements liés à un dispositif d'externalisation ou à un prestataire de services (p. ex. les changements liés à sa situation financière, à ses structures organisationnelles ou de participation, à la sous-externalisation) ;

   iii. l'examen et l'audit indépendants de la conformité avec les exigences et les politiques prévues par la réglementation en vigueur ;

   iv. le processus de renouvellement ;

e. les documents et la conservation d'informations, en tenant compte des exigences énoncées aux points 53 à 58 ;

f. les stratégies de sortie et les processus de résiliation, y compris l'exigence d'un plan de sortie documenté pour chaque fonction critique ou importante à externaliser lorsqu'une telle sortie est jugée possible compte tenu des éventuelles interruptions de service ou de la résiliation imprévue d'un accord d'externalisation, *conformément aux points 111 à 113*.

41. La politique d'externalisation doit établir une distinction entre les éléments suivants :

a. l'externalisation de fonctions critiques ou importantes et les autres dispositifs d'externalisation ;

b. l'externalisation à des prestataires de services agréés par une autorité compétente *pertinente dans un État membre ou un pays tiers* et l'externalisation à ceux qui ne le sont pas ;

c. les dispositifs d'externalisation intragroupe et l'externalisation à des entités extérieures au groupe ; et

d. l'externalisation à des prestataires de services situés dans un État membre ou dans un pays tiers.

42. Les Entités concernées doivent veiller à ce que la politique d'*externalisation* recense les effets potentiels suivants des dispositifs d'externalisation critiques ou importants et à ce que ceux-ci soient pris en compte dans le processus décisionnel :

a. le profil de risque des Entités concernées ;

b. la capacité à contrôler le prestataire de services et à gérer les risques ;

c. les mesures de poursuite de l'activité ; et

d. l'exercice de leurs activités commerciales.

Section 4.2.4 Conflits d'intérêts[22]

43. Les Entités concernées doivent identifier, évaluer et gérer les conflits d'intérêts liés à leurs dispositifs d'externalisation.

44. Lorsque l'externalisation donne lieu à des conflits d'intérêts importants, y compris entre entités du même groupe, les Entités concernées doivent prendre les mesures appropriées pour gérer ces conflits d'intérêts.

45. Lorsque les fonctions sont assurées par un prestataire de services faisant partie d'un groupe ou qui est détenu par l'Entité concernée ou par son groupe, les conditions, y compris les conditions financières, du service externalisé doivent être fixées dans des conditions de pleine concurrence. Toutefois, dans le cadre de la tarification des services, les synergies résultant de la fourniture de services identiques ou similaires à plusieurs Entités concernées peuvent être prises en compte, pour autant que le prestataire de services reste viable de

[22] *Veuillez vous référer également à la circulaire CSSF 12/552, Partie II, sous-chapitre 7.2 (points 165 à 174) pour les établissements de crédit ou à la circulaire CSSF 20/758, Partie II, sous-chapitre 7.2 (points 167 à 176) pour les entreprises d'investissement.*

manière autonome ; au sein d'un groupe, ce critère doit rester d'application indépendamment de la défaillance éventuelle de toute autre entité du groupe.

46. L'Entité concernée doit, en particulier, s'assurer que le prestataire de services est indépendant du réviseur d'entreprises agréé ou du cabinet de révision agréé en charge du contrôle légal des comptes de l'Entité concernée et du groupe auquel le réviseur d'entreprises agréé ou le cabinet d'audit agréé appartient.

Section 4.2.5 Plans de poursuite de l'activité

47. *Une attention particulière doit être accordée aux aspects de continuité et au caractère révocable d'un contrat d'externalisation. L'Entité concernée doit être en mesure de maintenir ses fonctions critiques en cas d'évènements exceptionnels ou de crises.*

48. Les Entités concernées doivent mettre en place, maintenir et tester périodiquement des plans appropriés de poursuite de l'activité pour les fonctions critiques ou importantes externalisées.

49. Les plans de poursuite de l'activité doivent tenir compte de l'éventualité selon laquelle la qualité de la fourniture de la fonction critique ou importante externalisée pourrait se dégrader de manière inacceptable ou être défaillante. Ces plans doivent également tenir compte de l'incidence potentielle de l'insolvabilité ou d'autres défaillances des prestataires de services et, le cas échéant, des risques politiques liés à la juridiction du prestataire de services.

50. *Lorsque le dispositif d'externalisation comprend des données et systèmes de TIC d'Entités concernées, les mesures relatives à la redondance et à la sauvegarde de ces systèmes et données doivent être spécifiées dans le contrat d'externalisation avec le prestataire de services ou configurées par les Entités concernées*[23]*, conformément au plan de continuité des activités des Entités concernées.*

Section 4.2.6 Fonction d'audit interne

51. Les activités de la fonction d'audit interne doivent couvrir, selon une approche fondée sur les risques, l'examen des activités externalisées. Le plan et le programme d'audit doivent comprendre, en particulier, la révision des dispositifs d'externalisation de fonctions critiques ou importantes.

52. En ce qui concerne le processus d'externalisation, la fonction d'audit interne doit au moins s'assurer :

[23] *En cas d'externalisation vers une infrastructure de cloud computing, le paramétrage des mesures de continuité peut être exécuté par les Entités concernées.*

a. que le cadre d'externalisation de l'Entité concernée, y compris la politique d'externalisation, est effectivement mis en œuvre et est conforme aux lois et règlements applicables, à la stratégie en matière de risques, ainsi qu'aux décisions de l'organe de direction ;

b. de l'adéquation, la qualité et l'efficacité de l'évaluation du caractère critique ou important des fonctions ;

c. de l'adéquation, la qualité et l'efficacité de l'évaluation des risques liés aux dispositifs d'externalisation et que ces risques restent conformes avec la stratégie de l'Entité concernée en matière de risques ;

d. que le niveau de participation des organes de gouvernance est approprié ; et

e. que le suivi et la gestion des dispositifs d'externalisation sont appropriés.

Section 4.2.7 Exigences en matière de documentation

53. Les Entités concernées doivent tenir à jour un registre comprenant des informations sur tous les dispositifs d'externalisation au *niveau individuel* et, le cas échéant, aux niveaux sous-consolidé et consolidé, comme indiqué au point 3, et doivent dûment documenter tous les dispositifs d'externalisation en vigueur, en faisant une distinction entre l'externalisation de fonctions critiques ou importantes et les externalisations portant sur d'autres fonctions. Les Entités concernées doivent conserver la documentation relative à des accords d'externalisation arrivés à échéance dans le registre ainsi que les pièces justificatives pendant une durée appropriée, *conformément à la législation luxembourgeoise*.

54. *Pour les besoins de la surveillance prudentielle*, le registre doit comprendre au moins les informations suivantes pour tous les dispositifs d'externalisation existants :

a. un numéro de référence pour chaque dispositif d'externalisation ;

b. la date de début et, le cas échéant, la prochaine date de renouvellement du contrat, la date de fin et/ou les délais de préavis pour le prestataire de services et pour l'Entité concernée ;

c. une brève description de la fonction externalisée, y compris les données qui sont externalisées et la confirmation (ou non) que des données à caractère personnel (p. ex. en indiquant oui ou non dans un champ de données séparé) ont été transférées ou si leur traitement est externalisé vers un prestataire de services ;

d. une catégorie attribuée par l'Entité concernée qui reflète la nature de la fonction visée au point c) (p. ex. *TIC*, fonction de contrôle *interne*), ce qui doit faciliter l'identification des différents types de dispositifs ;

e. le nom du prestataire de services, le numéro d'immatriculation de la société, l'identifiant de la personne morale (si disponible), le siège social et autres coordonnées pertinentes, ainsi que le nom de son entreprise mère (le cas échéant) ;

f. le(s) pays au sein duquel ou desquels le service sera exécuté, y compris la localisation (c.-à-d. le pays ou la région) des données ;

g. si (oui/non) la fonction externalisée est considérée comme critique ou importante, avec un bref résumé des raisons pour lesquelles la fonction externalisée est considérée comme critique ou importante *ou non* ;

h. en cas d'externalisation vers un prestataire de services en nuage, les modèles de services et de déploiement en nuage, c.-à-d. en cloud public/privé/hybride/communautaire, et la nature spécifique des données conservées et les lieux (c.-à-d. les pays ou régions) où ces données seront stockées ;

i. la date de la dernière évaluation du caractère critique ou important de la fonction externalisée.

55. Pour l'externalisation de fonctions critiques ou importantes, le registre doit comprendre les informations complémentaires suivantes :

a. les Entités concernées et autres entreprises incluses dans le périmètre de consolidation prudentielle, le cas échéant, qui ont recours à l'externalisation ;

b. si le prestataire de services ou le *sous-traitant* fait ou non partie du groupe ou s'il appartient aux Entités concernées du groupe ;

c. la date de l'évaluation des risques la plus récente et un bref résumé des principaux résultats ;

d. la personne ou l'organe de décision (p. ex. l'organe de direction) de l'Entité concernée qui a approuvé le dispositif d'externalisation ;

e. la législation applicable à l'accord d'externalisation ;

f. les dates des derniers audits et des prochains audits prévus, le cas échéant ;

g. le nom des éventuels sous-traitants auxquels des parties significatives d'une fonction critique ou importante sont sous-externalisées, y compris le pays où les sous-traitants sont enregistrés, où le service sera exécuté et, le cas échéant, le lieu (c.-à-d. le pays ou la région) où les données seront stockées ;

h. un résultat de l'évaluation de la substituabilité du prestataire de services (facile, difficile ou impossible), la possibilité de réinternaliser une fonction

critique ou importante dans l'Entité concernée, ou l'impact d'une interruption de la fonction critique ou importante ;

i. l'identification de prestataires de services alternatifs conformément au point h ;

j. si la fonction critique ou importante externalisée soutient ou non des opérations métier soumises à des exigences horaires pour leur fonctionnement ;

k. le coût budgétaire annuel estimé ;

l. la date de la notification préalable à l'autorité compétente conformément aux points 59 et 60, le cas échéant.

56. Les Entités concernées doivent mettre à la disposition de l'autorité compétente, à sa demande, soit le registre complet de tous les dispositifs d'externalisation existants, soit des parties déterminées de celui-ci, telles que des informations sur tous les dispositifs d'externalisation relevant de l'une des catégories visées au point 54(d) (p. ex. tous les dispositifs d'externalisation en matière de TIC).

57. Les Entités concernées doivent documenter de manière appropriée les évaluations effectuées en application des points 66 à 103 et les résultats de leur suivi continu (p. ex. les performances du prestataire de services, le respect des niveaux de service convenus, les autres exigences contractuelles et réglementaires, les mises à jour de l'évaluation des risques).

58. Les Entités concernées doivent mettre à la disposition de l'autorité compétente, à sa demande, toutes les informations nécessaires pour lui permettre d'assurer *sa* surveillance effective, y compris une copie de l'accord d'externalisation.

Section 4.2.8 Conditions de surveillance de l'externalisation

59. Une Entité concernée qui envisage d'externaliser une fonction critique ou importante[24] doit notifier au préalable ses plans à l'autorité compétente en utilisant les instructions et, le cas échéant, les formulaires disponibles sur le site Internet de la CSSF. Une telle notification doit être soumise au moins trois (3) mois avant que l'externalisation prévue entre en vigueur. Lorsque l'externalisation envisagée est prévue auprès d'un PSF de support luxembourgeois soumis aux articles 29-1 à 29-6 de la LSF, cette période de préavis est réduite à un (1) mois. Toute externalisation prévue qui n'aura pas

[24] *Une Entité concernée doit également notifier l'autorité compétente en cas de changements significatifs à des dispositifs d'externalisation existants (p. ex. lorsque de tels changements significatifs ont une incidence sur une fonction externalisée critique ou importante ou lorsqu'ils font qu'un dispositif d'externalisation devient critique ou important) sans délai indu.*

été notifiée endéans la période de notification précisée ci-dessus et/ou pour laquelle il n'aura pas été fait usage des instructions et, le cas échéant, des formulaires disponibles sur le site Internet de la CSSF, sera considérée comme non notifiée.

60. La notification est sans préjudice des mesures de surveillance ou de l'application de mesures contraignantes et/ou des sanctions administratives que l'autorité compétente pourrait prendre dans le cadre de sa surveillance continue, lorsque ces projets d'externalisation semblent ne pas être conformes au cadre légal et réglementaire applicable.

En tout état de cause, les Entités concernées demeurent pleinement responsables de leur conformité avec toutes les lois et tous les règlements pertinents relatifs aux projets d'externalisation.

61. *Dans le cas où des établissements de crédit* ou établissements de paiement *externaliseraient* des fonctions d'activités bancaires ou de services de paiement à un prestataire de services situé au Luxembourg ou dans un autre État membre, dans la mesure où l'exécution de cette fonction *nécessiterait* un agrément ou un enregistrement *lorsque de telles activités seraient exercées au Luxembourg, une telle externalisation ne pourra avoir lieu* que si l'une des conditions suivantes est remplie :

a. le prestataire de services est agréé ou enregistré par une autorité compétente *pertinente dans cet État membre* pour exercer ces activités bancaires ou ces services de paiement ; ou

b. le prestataire de services est, d'une autre manière, autorisé à exercer ces activités bancaires ou ces services de paiement conformément au cadre juridique national applicable.

62. *Dans le cas où les établissements de crédit* ou établissements de paiement *externaliseraient* des fonctions d'activités bancaires ou de services de paiement à un prestataire de services situé dans un pays tiers, dans la mesure où l'exécution de cette fonction *nécessiterait* un agrément ou un enregistrement *lorsque de telles activités seraient exercées au Luxembourg, une telle externalisation ne pourra avoir lieu* que si les conditions suivantes sont remplies :

a. le prestataire de services est agréé ou enregistré pour fournir cette activité bancaire ou ce service de paiement dans le pays tiers et est surveillé par une autorité compétente pertinente dans ce pays tiers (ci-après dénommée « autorité de surveillance ») ; et

b. il existe un accord de coopération approprié[25], p. ex. sous la forme d'un protocole d'accord ou d'un accord de coordination organisant un collège de supervision, entre l'autorité compétente et les autorités de surveillance chargées de la surveillance du prestataire de services. *Les Entités concernées doivent contacter la CSSF dans les phases précoces de leur externalisation envisagée afin de s'assurer que les accords de coopération entre la CSSF et l'autorité de surveillance du pays tiers sont ou peuvent être mis en place.*

63. Pour les besoins des points 61 et 62, l'externalisation de fonctions d'activités bancaires dans la mesure où l'exécution de cette fonction nécessiterait une autorisation ou un enregistrement lorsque de telles activités seraient exercées au Luxembourg doit s'appliquer lorsqu'un établissement de crédit[26] prévoit de procéder à l'externalisation d'une proportion significative de l'activité qui consiste en la réception de dépôts et d'autres fonds remboursables du public[27].

64. *L'externalisation à un prestataire de services situé au Luxembourg relative à des services soumis à une obligation d'autorisation conformément aux articles 29-1 à 29-6 de la LSF ne peut avoir lieu que si l'une des conditions suivantes est remplie :*

a. le prestataire de services est autorisé par la CSSF, conformément aux articles 29-1 à 29-6 de la LSF, à fournir de tels services ; ou

b. le prestataire de services est, d'une autre manière, autorisé à exécuter ces services, c.-à-d. il s'agit un établissement de crédit ou d'une entité soumise à l'article 1-1, paragraphe 2, point c), de la LSF qui fait partie d'un groupe auquel appartient l'Entité concernée et qui traite exclusivement des opérations de groupe.

Sous-chapitre 4.3 Processus d'externalisation

Section 4.3.1 Analyse préalable à l'externalisation

65. Avant de conclure un accord d'externalisation, les Entités concernées doivent :

[25] *Les accords de coopération peuvent prendre la forme d'un protocole d'accord (Memorandum of Understanding - MoU) ou d'un accord dédié conclu entre l'autorité compétente et une autorité de surveillance d'un pays tiers dans le contexte de la surveillance prudentielle d'une Entité concernée spécifique. Une liste des MoU signés par la CSSF est disponible sur le site Internet de la CSSF. Une liste des MoU signés par la BCE est disponible sur le site Internet de la BCE.*
[26] *Ou POST Luxembourg.*
[27] *Conformément à l'article 2, paragraphe 3, de la LSF, il est interdit aux personnes ou entreprises autres que des établissements de crédit d'exercer l'activité de réception de dépôts ou d'autres fonds remboursables du public.*

a. évaluer si l'accord d'externalisation de services concerne une fonction importante ou critique ;

b. évaluer si les conditions de surveillance de l'externalisation sont remplies ;

c. identifier et évaluer tous les risques pertinents du dispositif d'externalisation ;

d. effectuer les vérifications nécessaires à l'égard du prestataire de services potentiel ; et

e. identifier et évaluer les conflits d'intérêts que l'externalisation pourrait entraîner.

Sous-section 4.3.1.1 Évaluation des risques liés aux dispositifs d'externalisation

66. Les Entités concernées doivent évaluer l'incidence potentielle des dispositifs d'externalisation sur leurs *capacités et* risques opérationnels, tenir compte des résultats de l'évaluation lorsqu'ils décident si la fonction doit être externalisée vers un prestataire de services, et prendre les mesures appropriées pour éviter tout risque opérationnel supplémentaire indu avant de conclure des accords d'externalisation.

67. L'évaluation doit inclure, le cas échéant, des scénarios d'événements de risque potentiel, y compris des événements de risque opérationnel très élevé, *en particulier lorsque le dispositif d'externalisation se rapporte à une fonction critique ou importante de l'Entité concernée.* Dans le cadre de l'analyse de scénarios, les Entités concernées doivent évaluer l'impact potentiel de services défaillants ou inadéquats, y compris les risques causés par les processus, systèmes, personnes ou événements externes. Les Entités concernées doivent documenter l'analyse effectuée et ses résultats et estimer dans quelle mesure le dispositif d'externalisation augmenterait ou réduirait leur risque opérationnel. *Les entités de petite taille* peuvent utiliser des approches qualitatives d'évaluation des risques, tandis que les *autres* Entités concernées doivent adopter une approche plus sophistiquée, y compris, le cas échéant, l'utilisation de données internes et externes sur les pertes pour éclairer l'analyse du scénario.

68. Lorsqu'ils procèdent à l'évaluation des risques préalablement à la mise en place d'une externalisation et pendant le suivi continu des performances du prestataire de services, les Entités concernées doivent, au moins :

a. identifier et classifier les fonctions pertinentes et les données et systèmes connexes au regard de leur sensibilité *aux risques* et des mesures de sécurité requises ;

b. procéder à une analyse approfondie fondée sur les risques des fonctions et des données et systèmes connexes dont l'externalisation est envisagée ou qui ont été externalisés, *afin d'*examiner les risques potentiels, en

particulier les risques opérationnels, y compris les risques juridiques, de TIC, de conformité et de réputation, ainsi que les limites en matière de contrôle liées aux pays où les services externalisés sont ou pourraient être fournis et où les données sont stockées ou sont susceptibles de l'être ;

c. examiner les conséquences du lieu d'implantation du prestataire de services (à l'intérieur ou à l'extérieur de l'*EEE*) *conformément aux points 61 à 64 et si le prestataire de services est surveillé par une autorité compétente pertinente* ;

d. examiner la stabilité politique et la situation en matière de sécurité des juridictions en question, y compris :

   i. les lois en vigueur, et notamment les lois sur la protection des données ;

   ii. les dispositions en vigueur en matière d'application des lois ; et

   iii. les dispositions en vigueur en matière d'insolvabilité qui s'appliqueraient en cas de défaillance d'un prestataire de services et les contraintes qui pourraient apparaître en ce qui concerne la récupération urgente des données de l'Entité concernée en particulier ;

e. définir et décider d'un niveau approprié de protection de la confidentialité des données, de poursuite des activités externalisées, ainsi que d'intégrité et de traçabilité des données et des systèmes dans le cadre de l'externalisation *(*envisagée*)*. Les Entités concernées doivent également envisager la mise en place de mesures spécifiques, le cas échéant, applicables aux données en transit, aux données en mémoire et aux données au repos, telles que l'utilisation de technologies de cryptage associées à une architecture de gestion des clés appropriée ;

f. examiner si le prestataire de services est une filiale ou une entreprise mère de l'Entité concernée ou s'il est inclus dans le périmètre de consolidation comptable et, si tel est le cas, la mesure dans laquelle l'Entité concernée contrôle le prestataire de services ou peut exercer une influence sur ses actions.

69. Dans le cadre de l'évaluation des risques, les Entités concernées doivent également tenir compte des avantages et des coûts attendus du dispositif d'externalisation proposé, notamment en mettant en balance les risques qui pourraient être réduits ou mieux gérés avec les risques qui pourraient découler du dispositif d'externalisation proposé, en tenant compte au moins des éléments suivants :

a. les risques de concentration, y compris les risques provenant :

   i. de l'externalisation à un prestataire de services majeur qui n'est pas facilement substituable ; et

ii. d'accords d'externalisation multiples conclus avec le même prestataire de services ou des prestataires de services étroitement liés ;

b. les risques agrégés résultant de l'externalisation de plusieurs fonctions au sein de l'Entité concernée et, dans le cas de groupes d'Entités concernées, les risques agrégés sur une base consolidée ;

c. dans le cas d'Entités concernées importantes[28], le risque d'intervention (« step-in risk »), c'est-à-dire le risque qui peut résulter de la nécessité d'apporter un soutien financier à un prestataire de services en difficulté ou de reprendre ses activités commerciales ; et

d. les mesures mises en œuvre par l'Entité concernée et par le prestataire de services pour gérer et atténuer les risques.

70. Lorsque le dispositif d'externalisation prévoit la possibilité que le prestataire de services sous-traite des fonctions critiques ou importantes, *ou des parties significatives de celles-ci*, à d'autres prestataires de services, les Entités concernées doivent tenir compte :

a. des risques associés à la sous-externalisation, y compris les risques supplémentaires qui peuvent survenir si le sous-traitant est situé dans un pays tiers ou dans un pays autre que celui du prestataire de services ;

b. du risque que des chaînes longues et complexes de sous-externalisation réduisent la capacité des Entités concernées à contrôler la fonction critique ou importante externalisée et la capacité des autorités compétentes à les surveiller efficacement.

Sous-section 4.3.1.2 Diligence appropriée

71. Avant de conclure un accord d'externalisation et compte tenu des risques opérationnels liés à la fonction à externaliser, les Entités concernées doivent s'assurer, dans leur processus de sélection et d'évaluation, que le prestataire de services est apte à exercer la fonction en question.

72. Les Entités concernées doivent veiller à ce que le prestataire de services possède la réputation commerciale, des capacités appropriées et suffisantes, l'expertise, la capacité, les ressources (notamment humaines, TIC, financières), la structure organisationnelle et, le cas échéant, l'(les) autorisation(s) ou l'(les) enregistrement(s) réglementaire(s) nécessaire(s) pour exercer la fonction de manière fiable et professionnelle, de façon à satisfaire à ses obligations pendant toute la durée du projet de contrat.

[28] *En particulier les entités qui sont concernées par l'article 59-3 de la LSF.*

73. D'autres facteurs à prendre en considération lors de l'exercice d'une diligence appropriée à l'égard d'un prestataire de services potentiel comprennent notamment, mais sans limitation aucune :

a. le modèle d'entreprise, la nature, l'envergure, la complexité, la situation financière, ainsi que la structure de participation et du groupe du prestataire de services ;

b. les relations à long terme avec les prestataires de services qui ont déjà fait l'objet d'une évaluation et qui fournissent des services pour le compte de l'Entité concernée ;

c. si le prestataire de services est une entreprise mère ou une filiale de l'Entité concernée ou s'il est inclus dans le périmètre de consolidation comptable de l'Entité concernée ;

d. si le prestataire de services est ou non surveillé par des autorités compétentes *pertinentes*.

74. Lorsque l'externalisation implique le traitement de données à caractère personnel ou confidentielles, les Entités concernées doivent s'assurer que le prestataire de services met en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données.

75. Les Entités concernées doivent prendre les mesures appropriées pour veiller à ce que les prestataires de services agissent conformément à leurs valeurs et à leur code de conduite. En particulier, en ce qui concerne les prestataires de services situés dans des pays tiers et, le cas échéant, leurs sous-traitants, les Entités concernées doivent s'assurer que le prestataire de services agit d'une manière éthique et socialement responsable et respecte les normes internationales relatives aux droits de l'homme (p. ex. la Convention européenne des droits de l'homme), à la protection de l'environnement et à la mise en place de conditions de travail appropriées, notamment l'interdiction du travail des enfants.

Section 4.3.2 Phase contractuelle

76. Les droits et obligations de l'Entité concernée et du prestataire de services doivent être clairement répartis et définis dans un accord d'*externalisation* écrit.

77. *L'accord d'externalisation doit comporter les éléments suivants :*

a. une description claire de la fonction externalisée à fournir ;

b. la date de début et de fin de l'accord, le cas échéant, et les délais de préavis pour le prestataire de services et l'Entité concernée ;

c. la législation applicable à l'accord d'externalisation ;

d. les obligations financières des parties ;

e. si la sous-externalisation *notamment* d'une fonction critique ou importante, ou de parties significatives de celle-ci, est autorisée ou non et, dans l'affirmative, les conditions énoncées aux points 78 à 82 qui sont applicables à la sous-externalisation ;

f. le(s) lieu(x) (c.-à-d. les régions ou pays) où la fonction sera assurée et/ou où les données pertinentes seront conservées et traitées, y compris le lieu de stockage éventuel, et les conditions à remplir, y compris l'obligation d'informer l'Entité concernée si le prestataire de services envisage de modifier le(s) lieu(x) ;

g. le cas échéant, les dispositions concernant l'accessibilité, la disponibilité, l'intégrité, la confidentialité et la sécurité des données pertinentes, comme indiqué aux points 83 à 87 ;

h. le droit de l'Entité concernée de contrôler en permanence les performances du prestataire de services ;

i. les niveaux de service convenus, qui doivent inclure des objectifs de performance quantitatifs et qualitatifs précis pour la fonction externalisée afin de permettre un suivi en temps utile, de sorte que des mesures correctives appropriées puissent être prises dans les meilleurs délais si les niveaux de service convenus ne sont pas respectés ;

j. les obligations de reporting du prestataire de services envers l'Entité concernée, y compris la communication par le prestataire de services de tout fait nouveau susceptible d'avoir une incidence significative sur sa capacité à exercer efficacement la fonction selon les niveaux de service convenus et conformément aux lois et aux exigences réglementaires applicables *(y compris l'obligation de déclarer tout problème significatif ayant une incidence sur les fonctions externalisées, de même que toute situation d'urgence)* et, le cas échéant, l'obligation de présenter des rapports de la fonction de contrôle interne du prestataire de services ;

k. si le prestataire de services doit souscrire une assurance obligatoire contre certains risques et, le cas échéant, le niveau de couverture d'assurance demandé ;

l. l'obligation de mettre en œuvre et de tester les plans d'urgence de continuité de l'activité ;

m. des dispositions garantissant l'accès aux données appartenant à l'Entité concernée en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du prestataire de services ;

n. l'obligation pour le prestataire de services de coopérer avec les autorités compétentes et*, le cas échéant,* les autorités de résolution de l'Entité concernée, y compris avec les autres personnes désignées par celles-ci ;

o. pour les établissements *BRRD*, une référence claire aux pouvoirs de l'autorité nationale de résolution[29], en particulier aux articles 59-47 de la LSF et aux articles 66 et 69 de la Loi BRRD, et notamment une description des « obligations essentielles » du contrat au sens de l'article 59-47 de la LSF et de l'article 66 de la Loi BRRD ;

p. le droit inconditionnel des Entités concernées et des autorités compétentes d'inspecter et d'auditer le prestataire de services, *y compris en cas de sous-externalisation*, en ce qui concerne, *au moins*, la fonction critique ou importante externalisée, comme indiqué aux points 88 à 100 ;

q. les droits de résiliation, tels que précisés aux points 101 à 103.

Sous-section 4.3.2.1 Sous-externalisation

78. L'accord d'externalisation doit préciser si la sous-externalisation, *notamment* de fonctions critiques ou importantes, ou de parties significatives de celles-ci, est permise ou non.

79. Si la sous-externalisation de fonctions critiques ou importantes est autorisée, les Entités concernées doivent déterminer si la partie de la fonction à sous-externaliser est, en tant que telle, critique ou importante (c.-à-d. une partie significative de la fonction critique ou importante) et, si tel est le cas, elles doivent l'inscrire au registre.

80. Si la sous-externalisation de fonctions critiques ou importantes, *ou de parties significatives de celles-ci*, est permise, l'accord *d'externalisation* écrit doit :

a. préciser tous les types d'activités qui sont exclus de la sous-externalisation ;

b. préciser les conditions à respecter en cas de sous-externalisation ;

c. préciser que le prestataire de services est tenu de superviser les services qu'il a sous-externalisés afin de s'assurer que toutes les obligations contractuelles entre le prestataire de services et l'Entité concernée sont constamment respectées ;

d. exiger du prestataire de services qu'il obtienne au préalable l'autorisation écrite, spécifique ou générale de l'Entité concernée avant de sous-externaliser des données ;[30]

[29] *signifie une autorité telle que définie au point (8) de l'article 1er de la Loi BRRD.*

[30] *Voir l'article 28 du RGPD.*

e. prévoir l'obligation pour le prestataire de services d'informer l'Entité concernée de toute sous-externalisation prévue, ou de tout changement significatif concernant celle-ci, en particulier lorsque ce changement pourrait affecter la capacité du prestataire de services à s'acquitter des responsabilités qui lui incombent en vertu de l'accord d'externalisation. Cela inclut les changements significatifs prévus concernant les sous-traitants et le délai de notification ; en particulier, le délai de notification à fixer doit permettre à l'Entité concernée d'effectuer au moins une évaluation des risques liés aux changements proposés et de s'opposer aux changements avant que la sous-externalisation prévue, ou les changements significatifs concernant celle-ci, ne prenne(nt) effet ;

f. s'assurer, le cas échéant, que l'Entité concernée a le droit de s'opposer à la sous-externalisation envisagée, ou aux changements significatifs concernant celle-ci, ou qu'une approbation explicite est requise ;

g. s'assurer que l'Entité concernée a le droit contractuel de résilier l'accord en cas de sous-externalisation abusive, par exemple lorsque la sous-externalisation augmente sensiblement les risques pour l'Entité concernée, ou lorsque le prestataire de services sous-externalise les services sans en informer l'Entité concernée.

81. Les Entités concernées ne doivent accepter la sous-externalisation *de fonctions critiques ou importantes, ou de parties significatives de celles-ci,* que si le sous-traitant s'engage :

a. à se conformer à toutes les lois, exigences réglementaires et obligations contractuelles applicables ; et

b. à accorder à l'Entité concernée et à l'autorité compétente les mêmes droits contractuels d'accès et d'audit que ceux accordés par le prestataire de services.

82. Les Entités concernées doivent s'assurer que le prestataire de services contrôle de manière appropriée les *sous-traitants*, conformément à la politique définie par l'Entité concernée. Si la sous-externalisation proposée risque d'avoir des effets négatifs significatifs sur le dispositif d'externalisation d'une fonction critique ou importante ou d'entraîner une augmentation significative du risque, y compris lorsque les conditions énoncées au point 81 ne sont pas remplies, l'Entité concernée doit exercer son droit de s'opposer à la sous-externalisation, si ce droit a été convenu, et/ou de résilier le contrat.

Sous-section 4.3.2.2 Sécurité des données et des systèmes

83. *La confidentialité et l'intégrité des données et des systèmes doivent être maîtrisées dans toute la chaîne d'externalisation. Notamment, l'accès aux données et systèmes doit respecter les principes du « besoin de savoir » et du « moindre privilège » : l'accès n'est octroyé qu'aux personnes dont la fonction*

le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions.

84. Les Entités concernées doivent veiller à ce que les prestataires de services, le cas échéant, se conforment à des normes de sécurité *TIC* appropriées.

85. Le cas échéant (p. ex. dans le contexte de l'externalisation de services en nuage ou d'autres services TIC), les Entités concernées doivent définir les exigences de sécurité des données et des systèmes dans le cadre du dispositif d'externalisation et contrôler en permanence le respect de ces exigences. *Lorsque, dans le cadre de l'accord d'externalisation, des mesures de sécurité sont mises à disposition par le prestataire de services aux Entités concernées pour une sélection et une configuration personnalisées (notamment pour l'externalisation en nuage), les Entités concernées doivent veiller à ce qu'une sélection et une configuration correctes ont lieu, conformément à la politique et aux exigences en matière de sécurité de l'Entité concernée.*

86. Dans le cas de l'externalisation vers des fournisseurs de services en nuage et d'autres dispositifs d'externalisation qui impliquent le traitement ou le transfert de données à caractère personnel ou confidentielles, les Entités concernées doivent adopter une approche fondée sur les risques en ce qui concerne le(s) lieu(x) de stockage et de traitement des données (c.-à-d. le pays ou la région) *qui doit en particulier prendre en compte le point 101(c), (d) et (e)* et les considérations relatives à la sécurité informatique *et respecter les dispositions des points 133 à 142*.

87. Sans préjudice des exigences du *RGPD*, lorsqu'elles externalisent des services (en particulier vers des pays tiers), les Entités concernées doivent tenir compte des différences entre les dispositions nationales concernant la protection des données. Les Entités concernées doivent veiller à ce que l'accord d'externalisation prévoit l'obligation pour le prestataire de services de protéger les informations confidentielles, personnelles ou sensibles et de se conformer à toutes les exigences légales concernant la protection des données qui s'appliquent à l'Entité concernée (p. ex. protection des données à caractère personnel, respect du secret bancaire ou d'obligations de confidentialité similaires en ce qui concerne les informations sur les clients, le cas échéant).

Sous-section 4.3.2.3 Droits d'accès, d'information et d'audit

88. Les Entités concernées doivent s'assurer que dans l'*accord* d'externalisation écrit, la fonction d'audit interne, le *réviseur d'entreprises agréé et l'autorité compétente ont un accès garanti aux informations relatives aux activités externalisées* selon une approche fondée sur les risques *afin de leur permettre d'émettre une opinion fondée sur l'adéquation de l'externalisation. Cet accès inclut que les précités peuvent également vérifier les données pertinentes détenues par le prestataire de services et, dans les cas prévus par la législation nationale, ont le pouvoir de mener des contrôles sur place auprès du prestataire*

de services. L'opinion susmentionnée peut, le cas échéant, se baser sur les rapports du réviseur externe du prestataire de services. L'accord d'externalisation écrit doit aussi prévoir que les fonctions de contrôle interne ont accès à tout moment et sans encombre à toute documentation relative aux activités externalisées afin de maintenir en permanence la capacité de ces fonctions à exercer leurs contrôles.

89. Indépendamment du caractère critique ou important de la fonction externalisée, l'*accord* d'externalisation écrit doit faire référence aux pouvoirs de collecte d'informations et d'enquête des autorités compétentes en vertu *des articles 49, 53 et 59 de la LSF et des articles 31, 38 et 58-5 de la LSP* et*, le cas échéant,* des autorités de résolution *en vertu de l'article 61, paragraphe 1, de la Loi BRRD* en ce qui concerne les prestataires de services situés dans un État membre, et doit également garantir ces droits en ce qui concerne les prestataires de services situés dans des pays tiers.

90. En ce qui concerne l'externalisation de fonctions critiques ou importantes, les Entités concernées doivent veiller, dans l'accord d'externalisation écrit, à ce que le prestataire de services leur accorde, *à leurs réviseurs d'entreprises agréés* et à leur autorité compétente, y compris*, le cas échéant,* leur autorité de résolution, et à toute autre personne désignée par eux ou par l'autorité compétente *ou par l'autorité de résolution*, les droits suivants :

a. un accès complet à tous les locaux professionnels pertinents (p. ex. sièges sociaux et centres opérationnels), y compris à l'ensemble des appareils, systèmes, réseaux, informations et données pertinents utilisés pour assurer la fonction externalisée, notamment les informations financières connexes, le personnel et les auditeurs externes du prestataire de services (les « droits d'accès et d'information ») ; et

b. des droits inconditionnels en matière d'inspection et d'audit du dispositif d'externalisation (« droits d'audit »)*, y compris la possibilité pour l'autorité compétente de communiquer toute observation faite dans ce contexte aux Entités concernées,* afin de leur permettre de contrôler le dispositif d'externalisation et de s'assurer du respect *des* exigences réglementaires et contractuelles applicables.

91. En ce qui concerne l'externalisation de fonctions qui ne sont pas critiques ou importantes, les Entités concernées doivent garantir les droits d'accès et d'audit prévus au point 90 *et à la sous-section 4.3.2.3,* selon une approche fondée sur les risques, compte tenu de la nature de la fonction externalisée et des risques opérationnels et de réputation connexes, de son caractère évolutif, de l'incidence potentielle sur la poursuite de ses activités et de la durée du contrat. Les entités concernées doivent tenir compte du fait que les fonctions peuvent devenir critiques ou importantes au fil du temps.

92. Les Entités concernées doivent veiller à ce que l'accord d'externalisation ou toute autre disposition contractuelle n'entrave ni ne limite l'exercice effectif des droits d'accès et d'audit par elles-mêmes, *par les réviseurs d'entreprises agréés*, par les autorités compétentes ou par les tiers désignés par elles pour exercer ces droits.

93. Les Entités concernées doivent exercer leurs droits d'accès et d'audit, déterminer la fréquence des audits et les domaines à auditer selon une approche fondée sur les risques et se conformer à des normes d'audit nationales et internationales pertinentes et communément acceptées.

94. Sans préjudice de leur responsabilité finale en ce qui concerne les dispositifs d'externalisation, les Entités concernées peuvent avoir recours :

a. à des audits regroupés organisés conjointement avec d'autres clients du même prestataire de services, et réalisés par eux-mêmes et par les autres clients, ou par un tiers qu'ils auraient désigné, afin d'utiliser plus efficacement les ressources d'audit et de réduire la charge organisationnelle tant pour les clients que pour le prestataire de services ;

b. à des certifications de tiers et à des rapports d'audit internes ou externes mis à disposition par le prestataire de services.

95. En ce qui concerne l'externalisation de fonctions critiques ou importantes, les Entités concernées doivent évaluer si les certifications et les rapports visés au point 94(b), sont adéquats et suffisants pour se conformer à leurs obligations réglementaires et ne doivent pas se fier uniquement à ces rapports sur le long terme.

96. Les Entités concernées ne doivent recourir à la méthode visée au point 94(b), que si elles :

a. sont satisfaites du plan d'audit pour la fonction externalisée ;

b. veillent à ce que le périmètre de la certification ou du rapport d'audit couvre les systèmes (à savoir les processus, les applications, les infrastructures, les centres de données, etc.) et les contrôles considérés comme essentiels par l'Entité concernée, ainsi que le respect des exigences réglementaires pertinentes ;

c. évaluent de manière approfondie et continue le contenu des certifications ou des rapports d'audit, et s'assurent que les rapports ou les certifications ne sont pas obsolètes ;

d. s'assurent que les systèmes et contrôles essentiels sont couverts dans les futures versions de la certification ou du rapport d'audit ;

e. sont satisfaites de l'aptitude de la partie chargée de la certification ou de l'audit (notamment en ce qui concerne la rotation de l'entreprise chargée de la certification ou de l'audit, les qualifications, l'expertise, la

réexécution/la vérification des éléments probants inclus dans le dossier d'audit sous-jacent) ;

f. s'assurent que les certifications sont délivrées et que les audits sont effectués sur la base de normes professionnelles pertinentes largement reconnues et qu'ils incluent un test relatif à l'efficacité opérationnelle des contrôles essentiels en place ;

g. ont le droit contractuel de demander l'extension du périmètre des certifications ou des rapports d'audit à d'autres systèmes et contrôles pertinents ; le nombre et la fréquence de ces demandes de modification du périmètre doivent être raisonnables et légitimes du point de vue de la gestion des risques ; et

h. conservent le droit contractuel d'effectuer, à leur discrétion, des audits individuels en ce qui concerne l'externalisation de fonctions critiques ou importantes.

97. Les Entités concernées doivent, le cas échéant, s'assurer qu'elles sont en mesure d'effectuer des tests d'intrusion pour évaluer l'efficacité des mesures et des processus mis en œuvre en matière de cybersécurité et de sécurité des TIC internes.

98. Avant toute planification d'inspection sur place et dans un délai raisonnable, les Entités concernées, les auditeurs ou les tiers agissant au nom de l'Entité concernée ou de l'autorité compétente doivent en informer le prestataire de services, à moins que cela ne soit impossible en raison d'une situation d'urgence ou de crise ou ne conduise à une situation dans laquelle l'audit ne serait plus efficace.

99. Lors de la réalisation d'audits dans des environnements multi-clients, il convient de veiller à ce que les risques pour l'environnement d'un autre client (p. ex. l'impact sur les niveaux de service, la disponibilité des données, les aspects de confidentialité) soient évités ou atténués.

100. Lorsque le dispositif d'externalisation présente un niveau élevé de complexité technique, par exemple dans le cas de l'externalisation en nuage, l'Entité concernée doit s'assurer que la personne qui effectue l'audit – qu'il s'agisse de ses auditeurs internes, de l'équipe d'auditeurs ou des auditeurs externes agissant en son nom – possède les compétences et les connaissances appropriées et pertinentes pour procéder à un audit et/ou à une évaluation pertinents de manière efficace. Il en va de même pour tout membre du personnel de l'Entité concernée qui examine les certifications ou les audits effectués par les prestataires de services.

Sous-section 4.3.2.4 Droits de résiliation

101. L'*accord* d'externalisation doit expressément prévoir la possibilité pour l'Entité concernée de résilier l'accord, conformément à la législation applicable, y compris dans les situations suivantes :

a. lorsque le prestataire de *services* chargé d'assurer les fonctions externalisées contrevient aux dispositions légales, réglementaires ou contractuelles applicables ;

b. lorsque des obstacles susceptibles d'altérer les performances de la fonction externalisée sont identifiés ;

c. lorsqu'il se produit des changements significatifs concernant le dispositif d'externalisation ou le prestataire de services (p. ex. sous-externalisation ou changement de sous-traitants) ;

d. lorsqu'il existe des faiblesses concernant la gestion et la sécurité de données ou d'informations confidentielles, personnelles ou sensibles ; et

e. lorsque des instructions sont données par l'autorité compétente pour la surveillance de l'Entité concernée, par exemple dans le cas où l'autorité compétente n'est plus en mesure de surveiller efficacement l'Entité concernée du fait du dispositif d'externalisation.

102. L'*accord* d'externalisation doit faciliter le transfert de la fonction externalisée vers un autre prestataire de services ou la réinternalisation de la fonction dans l'Entité concernée, *chaque fois que la continuité ou la qualité de la prestation de services risque d'être compromise.* À cette fin, l'*accord* d'externalisation écrit doit :

a. définir clairement les obligations du prestataire de services existant, dans le cas d'un transfert de la fonction externalisée vers un autre prestataire de services ou de la réintégration de la fonction à l'Entité concernée, y compris le traitement des données ;

b. fixer une période de transition appropriée au cours de laquelle le prestataire de services, après la résiliation de l'accord d'externalisation, continuerait d'assurer la fonction externalisée afin de réduire le risque de perturbations ;

c. prévoir l'obligation pour le prestataire de services d'aider l'Entité concernée à assurer le transfert ordonné de la fonction en cas de résiliation de l'accord d'externalisation ; et

d. sans préjudice de la législation applicable, inclure un engagement de la part du prestataire de services de supprimer les données et systèmes de l'Entité concernée endéans une période de temps raisonnable lorsque l'accord est résilié.

103. L'accord d'externalisation ne doit pas contenir de clause de résiliation ou d'arrêt des prestations en raison d'une procédure de faillite, de gestion

contrôlée, de sursis de paiement, de concordat préventif de faillite ou autres procédures analogues. En particulier, dans le contexte des établissements BRRD, ne sont pas permises des clauses qui déclenchent la résiliation ou l'arrêt des prestations en raison d'actions de résolution, de mesures de réorganisation ou d'une procédure de liquidation tels que requis conformément à la Loi BRRD.

Section 4.3.3 Contrôle des fonctions externalisées

104. Les Entités concernées doivent effectuer le suivi permanent des performances des prestataires de services en ce qui concerne tous les dispositifs d'externalisation selon une approche fondée sur les risques, l'accent étant mis principalement sur l'externalisation de fonctions critiques ou importantes, en veillant notamment à garantir *la continuité des services fournis dans le cadre de l'accord et* la disponibilité, l'intégrité et la sécurité des données et des informations. Lorsque le risque, la nature ou l'ampleur d'une fonction externalisée a changé de manière significative, les Entités concernées doivent réévaluer le caractère critique ou important de cette fonction.

105. Les Entités concernées doivent faire preuve de la compétence, du soin et de la diligence nécessaires dans *la planification, la mise en œuvre,* le suivi et la gestion des dispositifs d'externalisation.

106. Les Entités concernées doivent régulièrement mettre à jour leur évaluation des risques conformément aux points 66 à 70 et informer périodiquement l'organe de direction des risques identifiés en ce qui concerne l'externalisation de fonctions critiques ou importantes.

107. Les Entités concernées doivent surveiller et gérer les risques internes de concentration auxquels elles sont confrontées en lien avec les dispositifs d'externalisation, compte tenu des points 66 à 70.

108. Les Entités concernées doivent veiller en permanence à ce que les dispositifs d'externalisation répondent à des normes d'exécution et de qualité appropriées conformément à leurs politiques, en mettant particulièrement l'accent sur les fonctions critiques ou importantes externalisées ; à cet effet, elles doivent :

a. s'assurer qu'elles reçoivent des rapports appropriés des prestataires de services ;

b. évaluer les performances des prestataires de services à l'aide d'outils tels que des indicateurs clés de performance, des indicateurs de contrôle clés, des rapports sur les prestations de services, l'autocertification ou des examens indépendants ; et

c. examiner toutes les autres informations pertinentes reçues du prestataire de services, y compris les rapports sur les mesures visant à assurer la continuité de l'activité, et les tester.

109. Les Entités concernées doivent prendre des mesures appropriées si elles constatent des lacunes dans l'exercice de la fonction externalisée. En particulier, les Entités concernées doivent assurer le suivi de toute indication selon laquelle les prestataires de services pourraient ne pas exercer la fonction critique ou importante externalisée d'une manière efficace ou conforme aux lois et aux exigences réglementaires applicables. Si des lacunes sont constatées, les Entités concernées doivent prendre les mesures correctives ou de redressement appropriées. Ces mesures peuvent notamment comprendre la résiliation de l'accord d'externalisation avec effet immédiat, si nécessaire.

110. Les Entités concernées[31] doivent informer l'autorité compétente *sans délai* des changements significatifs et/ou événements graves concernant leurs dispositifs d'externalisation qui pourraient avoir une incidence significative sur la poursuite de leurs activités commerciales*, afin de permettre à l'autorité compétente d'évaluer si une action réglementaire est requise*.

Section 4.3.4 Plans de sortie

111. Lorsqu'elles externalisent des fonctions critiques ou importantes, les Entités concernées doivent disposer d'un *plan* de sortie documenté qui soit conforme à leur politique d'externalisation ainsi qu'à leurs *stratégies de sortie et* leurs plans de continuité de l'activité, et qui prenne au moins en compte les éventualités suivantes :

a. la résiliation des accords d'externalisation ;

b. la défaillance du prestataire de services ;

c. la détérioration de la qualité de la fonction assurée et les perturbations réelles ou potentielles de l'activité dues à la fourniture inadéquate ou défaillante de la fonction ;

d. les risques significatifs découlant de la fourniture adéquate et continue de la fonction.

112. Les Entités concernées doivent s'assurer qu'elles sont en mesure de se retirer des accords d'externalisation sans que cela n'entraîne de perturbations dans leurs activités commerciales, sans limiter leur conformité aux exigences réglementaires et sans nuire à la continuité et à la qualité des services qu'elles fournissent aux clients. Pour ce faire, elles doivent :

a. élaborer et mettre en œuvre des plans de sortie complets, documentés et suffisamment testés, le cas échéant (p. ex. en effectuant une analyse des

[31] *Voir également la circulaire CSSF 21/787.*

éventuels coûts, incidences, ressources et conséquences en termes de délais du transfert d'un service externalisé vers un autre prestataire) ; et

b. définir des solutions alternatives et élaborer des plans de transition pour permettre à l'Entité concernée de retirer et de transférer des fonctions et des données externalisées du prestataire de services vers d'autres prestataires, ou de les réinternaliser, ou de prendre d'autres mesures garantissant la continuité de l'exercice de la fonction ou de l'activité commerciale critique ou importante, d'une manière contrôlée et suffisamment testée, en tenant compte des difficultés susceptibles de résulter de la localisation des données et en prenant les mesures nécessaires au maintien de la continuité des activités pendant la phase de transition.

113. Lors de l'élaboration de *plans* de sortie, les Entités concernées doivent :

a. définir les objectifs du plan de sortie ;

b. réaliser une analyse d'impact sur l'activité qui soit proportionnée au risque des processus, des services ou des activités externalisés, afin de déterminer les ressources humaines et financières nécessaires à la mise en œuvre du plan de sortie ainsi que le temps nécessaire pour procéder à la sortie du dispositif d'externalisation ;

c. attribuer des fonctions, des responsabilités et des ressources suffisantes pour la gestion des plans de sortie et des activités de transition ;

d. définir des critères de réussite de la transition des fonctions et des données externalisées ; et

e. définir les indicateurs à utiliser pour le suivi du dispositif d'externalisation (tel que prévu aux points 104 à 110), y compris des indicateurs fondés sur des niveaux de service inacceptables qui doivent déclencher la sortie.

Partie II - Exigences relatives aux dispositifs d'externalisation en matière de TIC

114. L'objectif de cette partie est de définir les exigences spécifiques qui s'appliquent dans le contexte de l'externalisation de services TIC (cloud ou non-cloud), et qui doivent être remplies en sus des exigences générales établies dans la partie I de la présente circulaire. Les dispositions suivantes contribuent à la

gestion saine et prudente, à la bonne organisation des Entités concernées et à la préservation de la sécurité de l'information des Entités concernées[32].

115. Les exigences définies dans la présente partie II ne s'appliquent pas à l'externalisation de nature métier ou administrative (aussi appelée *business process outsourcing*, c'est-à-dire aux dispositifs d'externalisation qui ne sont pas exclusivement relatifs aux TIC), même si ces dispositifs d'externalisation comportent eux-mêmes une externalisation en matière de TIC, c'est-à-dire que les systèmes de TIC sous-jacents font partie de cette externalisation de nature métier ou administrative.

116. Lorsque l'externalisation en matière de TIC, ou au moins un des sous-traitants en cas de sous-externalisation, repose sur une infrastructure de cloud computing telle que définie au point 1, les Entités concernées doivent se conformer aux exigences énoncées aux points 114 à 119, si applicable, ainsi qu'au chapitre 2 de la partie II. Dans le cas de dispositifs d'externalisation en matière de TIC autres que ceux reposant sur une infrastructure de cloud computing telle que définie au point 1, les Entités concernées doivent se conformer aux exigences énoncées aux points 114 à 119, si applicable, ainsi qu'au chapitre 1 de la partie II.

117. Dans le cas de sous-externalisation en matière de TIC, les exigences de cette partie (telles qu'applicables conformément au point 116) doivent s'appliquer à toute la chaîne d'externalisation.

118. Conformément au principe de proportionnalité, une Entité concernée peut, si motivé par des conclusions exhaustives et solides de l'évaluation de la criticité des fonctions et de l'analyse des risques, justifier la non-application des exigences énoncées dans les points suivants lorsque l'externalisation en matière de TIC n'est pas critique ou importante et qu'il est peu probable qu'elle le devienne :

a. point 103 : la continuité en cas de résolution ou réorganisation ou d'une autre procédure ; et

b. point 112(b) : le transfert des services lorsque la continuité de la prestation de services est menacée.

119. Il est rappelé aux Entités concernées que pour tout dispositif d'externalisation en matière de TIC, elles doivent :

a. s'assurer que l'accès aux données et systèmes respecte les principes du « besoin de savoir » et du « moindre privilège », c'est-à-dire que l'accès

[32] Comme prévu, entre autres, à l'article 5, paragraphe 1*bis,* de la LSF, l'article 17 de la LSF, l'article 11, paragraphe 2, de la LSP, au point 135 de la circulaire CSSF 18/698, à l'article 5, paragraphe 2, du règlement CSSF N° 10-04 et à l'article 57, paragraphe 2, du règlement délégué (UE) 231/2013.

n'est octroyé qu'aux personnes dont la fonction le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions ; et

b. s'assurer que l'accès aux données soumises au secret professionnel est accordé conformément à l'article 41, paragraphe 2*bis*, de la LSF ou à l'article 30, paragraphe 2*bis*, de la LSP, le cas échéant.

Chapitre 1. Dispositifs d'externalisation en matière de TIC autres que ceux reposant sur une infrastructure de cloud computing

120. Les exigences des points 59 et 60 s'appliquent aux dispositifs d'externalisation en matière de TIC concernés par le présent chapitre.

Sous-chapitre 1.1 Exigences applicables aux Entités concernées autres que les PSF de support autorisés conformément aux articles 29-3, 29-5 et 29-6 de la LSF et leurs succursales à l'étranger

121. Sans préjudice du point 119 ci-dessus, les Entités concernées peuvent externaliser leurs services de gestion/d'opération de systèmes de TIC :

a. au Luxembourg[33], uniquement auprès d'un établissement de crédit ou d'un professionnel du secteur financier agréé en tant que PSF de support conformément à l'article 29-3 de la LSF (opérateurs de systèmes informatiques et de réseaux de communication du secteur financier - « OSIRC ») ; la seule exception autorisée en vertu de l'article 1-1, paragraphe 2, point c, de la LSF est le recours à une entité du groupe auquel l'Entité concernée appartient et qui traite exclusivement des opérations du groupe ;

b. à l'étranger, à tout prestataire de services TIC, y compris une entité du groupe auquel appartient l'Entité concernée.

122. Les Entités concernées peuvent externaliser les services TIC autres que les services de gestion/d'opération de systèmes de TIC à tout prestataire de services TIC, y compris à une entité du groupe fournissant des services TIC ou à un PSF de support. De tels dispositifs d'externalisation doivent être mis en place conformément aux exigences énoncées au point 119 ci-dessus. En particulier, si le prestataire de services n'est pas autorisé à accéder aux données soumises au secret professionnel conformément à l'article 41, paragraphe 2*bis*,

[33] Conformément à la LSF, l'opération de systèmes de TIC pour les établissements de crédit, professionnels du secteur financier, établissements de paiement, établissements de monnaie électronique, OPC, fonds de pension, entreprises d'assurance ou de réassurance de droit luxembourgeois ou étranger est une activité régulée qui nécessite une autorisation pour pouvoir être exercée au Luxembourg.

de la LSF ou à l'article 30, paragraphe 2*bis,* de la LSP, le cas échéant, le prestataire de services peut avoir accès à ces données seulement s'il est supervisé, tout au long de sa mission, par une personne de l'Entité concernée en charge des TIC.

Sous-chapitre 1.2 Exigences applicables aux PSF de support autorisés conformément aux articles 29-3, 29-5 et 29-6 de la LSF et à leurs succursales à l'étranger

123. Pour les besoins exclusifs du présent sous-chapitre, on entend par :

a. PSF de support : une Entité concernée, y compris ses succursales, qui est autorisée à exercer des activités OSIRC[34] conformément à l'article 29-3 ou des activités PSDC[35] conformément aux articles 29-5 ou 29-6 de la LSF ;

b. Systèmes de TIC propres[36] [37]: : les systèmes de support de l'organisation et de l'administration des PSF de support ; ils ne sont pas proposés en tant que service à des tiers et ne sont pas utilisés dans le cadre des services proposés à des tiers ;

c. Systèmes de TIC client : les systèmes qui remplissent les deux conditions cumulatives suivantes :

   i. ils supportent partiellement ou exclusivement les activités prestées pour les clients régulés du secteur financier des PSF de support, indépendamment de leur appartenance au client ou au PSF de support ou de leur localisation ; et

   ii. le PSF de support est responsable envers son client de leur bon fonctionnement.

124. Sans préjudice du point 119 ci-dessus, les PSF de support et leurs succursales autorisés en tant qu'OSIRC conformément à l'article 29-3 de la LSF peuvent partiellement externaliser leurs services d'opérateur de TIC, c'est-à-dire certains services de gestion/d'opération de systèmes de TIC client[38] pour autant que les conditions prévues aux points 126 et 127 sont remplies.

125. Sans préjudice du point 119 ci-dessus, les PSF de support et leurs succursales autorisés en tant que PSDC conformément à l'article 29-5 ou à

[34] Opérateurs de systèmes informatiques et de réseaux de communication du secteur financier (« OSIRC »).
[35] Prestataires de services de dématérialisation et/ou de conservation du secteur financier (« PSDC »).
[36] Le terme « système » peut ici se limiter à un logiciel si le service concerne uniquement un logiciel.
[37] À titre d'exemple (liste non-exhaustive) : les systèmes de comptabilité, de gestion du personnel et de paiement du PSF de support ; les systèmes de gestion des commandes clients, de gestion des achats, de gestion de la relation client mais aussi les serveurs de messagerie, serveurs de fichiers internes, site Internet du PSF de support (hors utilisation pour des services prestés à ses clients), postes de travail du personnel, stockage de documents, téléphonie VoIP, etc.
[38] Une telle externalisation par un OSIRC est en fait une sous-externalisation du point de vue des Entités concernées qui externalisent vers cet OSIRC.

l'article 29-6 de la LSF peuvent partiellement externaliser leurs services de gestion/d'opération de systèmes de TIC qui supportent partiellement ou exclusivement les services de dématérialisation ou de conservation qu'ils fournissent à des clients régulés du secteur financier pour autant que les conditions prévues aux points 126 et 127 sont remplies.

126. Pour les dispositifs d'externalisation visés aux points 124 et 125 ci-dessus, le prestataire de services doit être :

a. au Luxembourg[39], uniquement un établissement de crédit ou une entité qui est autorisée en tant que PSF de support conformément à l'article 29-3 de la LSF ;
b. à l'étranger, tout prestataire de services TIC, y compris une entité du groupe auquel appartient le PSF de support.

127. Les dispositifs d'externalisation visés aux points 124 et 125 ci-dessus doivent être considérés comme critiques ou importants et sont interdits s'ils ne respectent pas ce qui suit :

a. La prestation de services est complémentaire[40] et ne vide pas le PSF de support (ou sa succursale, le cas échéant) de sa substance conformément au point 7 ;
b. Les PSF de support et leurs succursales ont obtenu l'accord préalable de tous leurs clients régulés du secteur financier concernés ;
c. Si le prestataire de services peut avoir accès aux données soumises au secret professionnel conformément à l'article 41 de la LSF ou à l'article 30 de la LPS, le cas échéant, les PSF de support et leurs succursales ont informé de manière claire leurs clients régulés du secteur financier et ont obtenu leur consentement préalable ;
d. Chaque année, les PSF de support et leurs succursales doivent fournir à l'autorité compétente leur plan de contrôle détaillé et leur plan de sortie afin d'assurer le respect des sections 4.3.3 et 4.3.4 de la présente circulaire ;
e. Les PSF de support et leurs succursales ont obtenu l'accord préalable de l'autorité compétente pour une telle externalisation en utilisant les instructions et, le cas échéant, les formulaires disponibles sur le site Internet de la CSSF.

[39] Conformément à la LSF, l'opération de systèmes de TIC pour les établissements de crédit, professionnels du secteur financier, établissements de paiement, établissements de monnaie électronique, OPC, fonds de pension, entreprises d'assurance ou de réassurance de droit luxembourgeois ou étranger est une activité régulée qui nécessite une autorisation pour pouvoir être exercée au Luxembourg.
[40] Un exemple de complémentarité est l'opération d'un logiciel par un OSIRC (ou de sa succursale, le cas échéant) et l'opération en cascade de l'infrastructure sous-jacente par un prestataire de services.

128. Sans préjudice des points 59, 60 et 119 ci-dessus, les PSF de support et leurs succursales peuvent externaliser les services de gestion/d'opération de leurs propres systèmes de TIC :

a. au Luxembourg, uniquement auprès d'un établissement de crédit ou d'une entité qui est autorisée en tant que PSF de support conformément à l'article 29-3 de la LSF ;

b. à l'étranger, auprès de tout prestataire de services TIC, y compris à une entité du groupe auquel appartient le PSF de support.

129. La prestation de services d'opération de TIC relatifs à des systèmes de TIC client ou des systèmes supportant les activités des PSDC, par les succursales de PSF de support à leur siège, est interdite si les services ne sont pas conformes aux exigences pertinentes établies au point 127.

130. Les PSF de support et leurs succursales agissant en qualité d'OSIRC peuvent recourir, pour leurs prestations d'opérateurs de TIC, à des infrastructures appartenant à leur groupe, à condition que les services prestés par le groupe ou leurs éventuels sous-traitants, soient limités à ceux nécessitant une présence physique sur ces infrastructures. La gestion des systèmes contenant les données et les traitements à charge du PSF de support doit être exclue d'une telle externalisation. Par infrastructure, il faut comprendre les ressources informatiques nécessaires à l'hébergement des systèmes et des données dont l'OSIRC a la gestion. Dans ce cas, les PSF de support doivent, en particulier, veiller à garder un contrôle permanent sur les actions réalisées par le groupe pour leur compte. Lorsque cette externalisation implique la présence, sur les infrastructures, de données soumises au secret professionnel conformément à l'article 41 de la LSF ou à l'article 30 de la LPS, le cas échéant, les PSF de support doivent obtenir l'accord préalable des clients régulés du secteur financier avant de procéder à l'externalisation.

131. Les succursales des PSF de support peuvent proposer à leurs clients régulés du secteur financier du pays où elles sont établies (« pays d'accueil ») des services reposant sur une infrastructure établie dans le pays d'accueil. Cette infrastructure peut être externalisée à un prestataire de services local à condition que les services prestés par ce prestataire et ses éventuels sous-traitants, soient limités à ceux nécessitant une présence physique sur ces infrastructures et à l'exclusion de toute gestion des systèmes contenant les données et traitements à charge du PSF de support ou de sa succursale. La succursale doit appliquer les principes énoncés dans la présente circulaire et le siège au Luxembourg doit conserver le contrôle adéquat des prestations réalisées par sa succursale. Les succursales doivent obtenir l'accord des clients régulés du secteur financier concernés pour cette externalisation locale.

132. Les PSF de support peuvent externaliser tout service de TIC autre que les services visés aux points 124 à 131 ci-dessus à tout prestataire de services TIC,

y compris à une entité du groupe fournissant des services TIC ou à un PSF de support. De tels dispositifs d'externalisation doivent être mis en place conformément aux exigences énoncées au point 119 ci-dessus. En particulier, si le prestataire de services n'est pas autorisé à accéder aux données soumises au secret professionnel conformément à l'article 41 de la LSF ou à l'article 30 de la LSP, le cas échéant, le prestataire de services peut avoir accès à ces données seulement s'il est supervisé, tout au long de sa mission, par une personne du PSF de support en charge des TIC.

Chapitre 2. Dispositifs d'externalisation en matière de TIC reposant sur une infrastructure de cloud computing

133. Le présent chapitre établit des exigences spécifiques supplémentaires à respecter en cas d'externalisation en matière de TIC reposant sur une infrastructure de cloud computing (ci-après également « solutions de cloud computing »). L'utilisation d'un cloud privé sans recours à une externalisation est donc exclue du champ d'application de ce chapitre.

Sous-chapitre 2.1 Définitions et application

Section 2.1.1 Terminologie spécifique

134. Pour les besoins de ce chapitre et en sus des définitions fournies au point 1, les définitions suivantes s'appliquent :

1) Interface client	désigne la couche logicielle mise à disposition par le fournisseur de services de cloud computing à l'Entité concernée pour lui permettre de gérer ses ressources de cloud computing.
2) Ressource de cloud computing	désigne toute capacité informatique (p. ex. serveur, stockage, réseau, etc.) mise à disposition par un fournisseur de services de cloud computing.
3) Fournisseur de services de cloud computing	désigne toute entreprise proposant des services de cloud computing correspondant à la définition de ce chapitre 2.
4) Entité concernée	désigne une Entité concernée telle que définie au point 2, consommant des ressources de cloud computing pour les besoins du fonctionnement de ses activités.
5) Multi-tenant	qualifie une infrastructure matérielle ou logicielle permettant de servir plusieurs

	Entités (concernées) via des ressources de cloud computing partagées et à l'aide d'un modèle standardisé.
6) Opération des ressources	désigne le fait de gérer les ressources de cloud computing 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 de cloud computing.

Section 2.1.2 Définition de « cloud computing »

135. Le cloud computing est un modèle composé des cinq caractéristiques essentielles suivantes[41] :

a. Libre-service et à la demande : Une Entité concernée[42] 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 de cloud computing.

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

c. Ressources partagées : Les ressources informatiques du fournisseur de services de cloud computing sont partagées afin de servir les multiples Entités (concernées) dans un modèle « multi-tenant ». Les ressources physiques et virtuelles sont dynamiquement allouées et réaffectées en fonction des demandes des Entités concernées. L'Entité concernée n'a pas de contrôle ou pas la connaissance quant à l'emplacement exact de la ressource mise à disposition, il peut néanmoins contrôler ou connaître l'emplacement à un niveau d'abstraction plus élevé (p. ex. le pays, la région ou le centre de données). Ces ressources informatiques partagées incluent,

[41] La CSSF se réfère aux définitions proposées par des organisations internationales telles que le NIST (National Institute of Standards and Technology - Institut national des normes et de la technologie) ou l'ENISA (European Union Agency for Cybersecurity - Agence de l'Union européenne pour la cybersécurité).

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

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 concernée, 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 de cloud computing contrôlent et optimisent automatiquement l'utilisation des ressources en exploitant un indicateur de capacité à un niveau d'abstraction approprié au type de service (p. ex. 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 concernée, assurant ainsi la transparence quant au service utilisé.

Section 2.1.3 Conditions d'application du chapitre 2

136. Une externalisation est considérée comme une « externalisation sur une infrastructure de cloud computing » au sens de la présente circulaire et soumise aux exigences du chapitre 2 lorsque les cinq caractéristiques essentielles définies au point 135 et les deux exigences spécifiques suivantes sont remplies :

a. Le personnel travaillant pour le fournisseur de services de cloud computing ne peut en aucun cas accéder aux données et aux systèmes qu'une Entité concernée détient sur l'infrastructure de cloud computing sans avoir obtenu au préalable l'accord explicite de l'Entité concernée et sans qu'un mécanisme de surveillance ne soit mis à la disposition de l'Entité concernée pour contrôler les accès réalisés. Ces accès doivent rester exceptionnels. L'accès peut cependant 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 (concernées) du fournisseur de services de cloud computing[43]. Tous les accès du fournisseur de services de cloud computing 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 de cloud computing n'engendre aucune interaction manuelle de la part du fournisseur de services pour la gestion quotidienne des ressources de cloud computing utilisées par l'Entité concernée[44] (p. ex. le provisionnement, la configuration ou la libération de ressources de cloud

[43] Dans ce cas d'extrême urgence, il conviendra de prévenir les Entités concernées a posteriori.
[44] C'est en effet un système automatisé qui permet de provisionner les ressources, d'où le point a) spécifiant que le personnel ne peut accéder par défaut aux ressources de l'Entité concernée.

computing). Ainsi, seul l'opérateur des ressources (qui est soit l'Entité concernée, soit un tiers autre que le fournisseur de services de cloud computing) gère son environnement de TIC hébergé sur l'infrastructure de cloud computing. Le fournisseur de services de cloud computing peut néanmoins intervenir manuellement :

i. pour la gestion globale des systèmes de TIC supportant l'infrastructure cloud (p. ex. maintenance du matériel physique, déploiement de nouvelles solutions non spécifiques à l'Entité concernée) ; ou

ii. dans le cadre d'une demande particulière de l'Entité concernée (p. ex. pour provisionner une ressource de cloud computing absente du catalogue proposé par le fournisseur ou insuffisante en performance).

Sous-chapitre 2.2 Les exigences à respecter pour une externalisation sur une infrastructure de cloud computing

137. Conformément au principe de proportionnalité, l'Entité concernée peut, si motivé par des conclusions exhaustives et solides de l'évaluation de la criticité des fonctions et de l'analyse des risques, justifier la non-application des exigences énoncées dans les points suivants de la présente circulaire lorsque les activités externalisées à une infrastructure de cloud computing ne sont pas liées à une fonction critique ou importante et qu'il est peu probable qu'elles le deviennent :

a. point 142(c) : notification de la part du fournisseur de services de cloud computing en cas de changement de fonctionnalités ;

b. point 142(d) : notification de la part de l'opérateur des ressources en cas de changement de fonctionnalités.

138. L'Entité concernée peut externaliser l'« opération des ressources » telle que définie au point 134 à un tiers lorsque ce tiers se trouve dans l'une des deux situations suivantes :

a. Le tiers est autorisé en tant qu'OSIRC conformément à l'article 29-3 de la LSF. Les PSF de support doivent également respecter les exigences de ce chapitre lorsque l'opération des ressources est effectuée pour une entité qui n'est pas un client régulé du secteur financier.

b. Le tiers n'est pas autorisé en tant qu'OSIRC conformément à l'article 29-3 de la LSF, soit parce qu'il est localisé à l'étranger ou parce qu'il s'agit d'une entité du groupe auquel appartient l'Entité concernée, qui est basée au Luxembourg et qui fournit des services opérationnels exclusivement au sein du groupe tel que stipulé à l'article 1-1, paragraphe 2, point c), de la LSF. Dans ce cas, en plus de respecter les exigences décrites dans la présente circulaire, l'Entité concernée doit effectuer une analyse de risques préalable et approfondie sur les activités de l'opérateur des ressources, notamment en vérifiant que les points suivants ont été correctement adressés :

i. les rôles et responsabilités définis entre l'opérateur des ressources et le fournisseur de services de cloud computing ;

ii. la gestion de l'isolation des environnements multi-tenants ;

iii. les indicateurs recueillis par l'opérateur des ressources pour surveiller les systèmes et données sur l'infrastructure de cloud computing ;

iv. les mesures de sécurité techniques et organisationnelles en place pour accéder aux interfaces clients afin de gérer les ressources de cloud computing, y compris la gestion des accès à l'interface client ;

v. la cohérence des politiques d'opérations et de sécurité définies par l'opérateur des ressources avec les configurations des ressources de cloud computing et les mesures de sécurité prévues ;

vi. les compétences des opérateurs (p. ex. certifications, formations techniques) ;

vii. la revue des rapports d'audit du fournisseur de services de cloud computing par l'opérateur des ressources ;

viii. le droit de l'autorité compétente et de l'Entité concernée d'auditer l'opérateur de ressources (en ligne avec les exigences définies aux points 88 à 100).

139. Il convient de préciser qu'une Entité concernée qui se repose sur un fournisseur de services qui cumule les activités de fournisseur de services de cloud computing et d'opérateur de ressources est soumise aux exigences du chapitre 2 à condition que ces deux activités soient proprement ségréguées (c.-à-d. de manière à ce que le personnel exerçant la fonction de fournisseur de services de cloud computing ne puisse pas accéder aux données et rester ainsi en conformité avec la définition de cloud computing au sens de ce chapitre). Ceci est également valable lorsque le fournisseur de services qui cumule les deux activités est autorisé conformément à l'article 29-3 de la LSF. Si cette exigence de ségrégation ne peut être remplie, l'externalisation n'est pas considérée comme une externalisation reposant sur une infrastructure de cloud computing au sens de ce chapitre mais comme une externalisation en matière de TIC classique ; dans un tel cas, seules les exigences du chapitre 1 de la partie II s'appliquent.

140. **« Cloud officer »**

a. L'opérateur des ressources doit désigner parmi ses employés une personne, le « cloud officer », qui a pour responsabilité l'utilisation des services de cloud computing et qui est garant des compétences du personnel gérant les ressources de cloud computing (voir point 142(a)). L'opérateur des ressources veille à attribuer la fonction de « cloud officer » à une personne qualifiée et maîtrisant les enjeux d'une externalisation sur une infrastructure de cloud computing. Cette fonction peut être exercée par des

personnes cumulant déjà d'autres fonctions au sein du département informatique.

b. Si l'opération des ressources est exercée par l'Entité concernée, il est possible que le « cloud officer » puisse cumuler pour responsabilité la gestion de la relation d'externalisation. Si l'Entité concernée fait appel à un tiers pour l'opération des ressources de cloud computing, l'Entité concernée devra connaître le nom du « cloud officer » de l'opérateur des ressources.

141. **Nécessité d'informer l'autorité compétente :**

a. Les exigences de notification des points 59 et 60 s'appliquent également aux dispositifs d'externalisation reposant sur une infrastructure de cloud computing. Pour le cas particulier où une entité autorisée conformément à l'article 29-3 de la LSF agit en tant qu'intermédiaire et non pas en tant qu'opérateur des ressources entre une Entité concernée et un fournisseur de services de cloud computing, l'Entité concernée doit soumettre une notification au moins trois (3) mois avant la mise en œuvre effective de l'externalisation prévue pour l'externalisation de fonctions critiques ou importantes au fournisseur de services de cloud computing.

b. Une entité autorisée en tant qu'OSIRC conformément à l'article 29-3 de la LSF doit demander l'autorisation de l'autorité compétente avant de procéder à la commercialisation dans les cas suivants :

   i. l'entité a l'intention d'agir en tant qu'opérateur des ressources pour ses clients régulés du secteur financier ;

   ii. l'entité a l'intention de fournir une infrastructure cloud à ses clients régulés du secteur financier, agissant ainsi en tant que fournisseur de services de cloud computing ;

   iii. l'entité a l'intention de fournir une solution de cloud computing à ses clients régulés du secteur financier, en s'appuyant sur une ou plusieurs infrastructures cloud. Cette entité agit alors en tant que fournisseur de services de cloud computing qui sous-externalise.

c. Sans préjudice du point 119, les PSF de support et leurs succursales autorisés en tant qu'OSIRC conformément à l'article 29-3 de la LSF peuvent partiellement externaliser leurs services d'opérateur des ressources[45] à condition de respecter le point 126 et les exigences énoncées au point 127. Dans un souci de clarté, une autorisation préalable par l'autorité compétente est de ce fait requise comme indiqué au point 127(e). Le point

[45] *Une telle externalisation par un OSIRC est en fait une sous-externalisation du point de vue des Entités concernées qui externalisent vers cet OSIRC.*

129 s'applique mutatis mutandis à la prestation de services d'opérateur de ressources.

142. **Gestion des risques d'externalisation :**

a. En ligne avec le point 35, l'opérateur des ressources doit conserver l'expertise nécessaire pour contrôler efficacement les prestations ou les tâches externalisées sur une infrastructure de cloud computing et gérer les risques associés à cette externalisation. En outre, l'opérateur des ressources doit s'assurer que le personnel en charge de la gestion des ressources de cloud computing, y compris le « cloud officer », dispose des compétences suffisantes pour assurer ses fonctions sur base de formations appropriées sur la gestion et la sécurité des ressources de cloud computing spécifiques au fournisseur de services de cloud computing.

b. Telle que prévue aux points 66 à 70, une évaluation des risques des dispositifs d'externalisation doit être effectuée par l'Entité concernée. Les risques spécifiques à l'utilisation de technologies de cloud computing doivent aussi faire partie de cette évaluation et comprendre, entre autres : le défaut d'isolation des environnements multi-tenants, les différentes législations applicables (pays de stockage des données et pays d'établissement du fournisseur de services de cloud computing), l'interception des données en transit, la défaillance des télécommunications (p. ex. la connexion Internet), l'utilisation du cloud comme « shadow IT »[46], le manque de portabilité des systèmes une fois ceux-ci déployés sur une infrastructure de cloud computing ou la défaillance de la continuité des services de cloud computing ;

c. Toute modification des fonctionnalités des applications par le fournisseur de services de cloud computing – autres que des modifications liées à la maintenance corrective – doit être communiquée à l'opérateur des ressources, préalablement à sa mise en production, qui doit en informer l'Entité concernée, afin que ceux-ci puissent prendre les mesures nécessaires en cas de changement majeur ou de discontinuité :

d. Toute modification des fonctionnalités des applications gérées par l'opérateur de ressources – autres que des modifications liées à la maintenance corrective – doit être communiquée à l'Entité concernée, préalablement à sa mise en production, afin que celle-ci puisse prendre les mesures nécessaires en cas de changement majeur ou de discontinuité ;

[46] Le « shadow IT » est l'utilisation des ressources de TIC non maîtrisée par le département informatique.

e. L'Entité concernée et l'opérateur des ressources doivent avoir pleinement conscience des éléments de continuité et de sécurité qui restent à leurs charges respectives lors du recours à une solution de cloud computing ;

f. L'Entité concernée doit comprendre les risques liés à une infrastructure de cloud computing et l'opérateur des ressources doit les maîtriser ;

g. L'Entité concernée et l'opérateur des ressources doivent savoir à tout moment où se trouvent globalement[47] leurs données et systèmes, qu'il s'agisse aussi bien des environnements de production que des réplications ou sauvegardes.

[47] Il est important que l'Entité concernée et l'opérateur des ressources sachent dans quels pays se trouvent les données, cela de manière globale. Par exemple, les données sont réparties entre le pays A et le pays B, mais ne peuvent en aucun cas être dans le pays C.

Commission de Surveillance du Secteur Financier

Partie III - Date d'application

143. La présente circulaire s'applique à compter du *30 juin 2022* à tous les accords d'externalisation conclus, révisés ou modifiés à cette date ou *après cette date*.

144. Les Entités concernées doivent réviser et modifier les accords d'externalisation existants en vue d'assurer qu'ils sont conformes à la présente circulaire.

145. Les Entités concernées doivent compléter la documentation de tous les accords d'externalisation en ligne avec la présente circulaire après la première date de renouvellement de chaque accord d'externalisation, mais au plus tard le *31 décembre 2022*.

Dans les cas où *les Entités concernées estiment que* la révision *et la modification* des accords d'externalisation de fonctions importantes ou critiques e*xistant avant le 30 juin 2022* ne *seront* pas achevées au *31 décembre 2022*, *elles* doivent en informer leur autorité compétente *en temps utile*, y compris les mesures prévues pour conclure la révision ou l'éventuelle stratégie de retrait.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Commission de Surveillance du Secteur Financier

Annexe - Liste des Orientations des ESA mises en œuvre

La présente circulaire met en œuvre :

- les Orientations révisées de l'EBA relatives à l'externalisation (**EBA/GL/2019/02)** ;
- les Orientations de l'ESMA relatives à la sous-traitance à des prestataires de services en nuage (**ESMA50-164-4285**, les **Orientations Cloud de l'ESMA**), auparavant mises en œuvre par la circulaire CSSF 21/777 modifiant la circulaire CSSF 17/654.

Les Orientations susmentionnées sont disponibles sur les sites Internet de l'EBA (www.eba.europa.eu) et de l'ESMA (www.esma.europa.eu).

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