EBA/GL/2019/02

25 février 2019

Orientations relatives à l'externalisation

1. Obligations de conformité et de déclaration

Statut de ces orientations

1. Le présent document contient des orientations adoptées en application de l'article 16 du règlement (UE) n° 1093/2010[1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes et les établissements financiers doivent tout mettre en œuvre pour respecter ces orientations.

2. Les présentes orientations exposent l'opinion de l'ABE concernant les pratiques de surveillance appropriées au sein du système européen de surveillance financière ou les modalités d'application de la législation de l'Union dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) nº 1093/2010, qui sont soumises aux orientations devraient s'y conformer en les intégrant dans leurs pratiques, s'il y a lieu (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations s'adressent en priorité à des établissements et à des établissements de paiement.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles se conforment ou entendent se conformer à ces orientations, ou indiquer, le cas échéant les raisons de la non-conformité à ces orientations, avant le ([jj.mm.aaaa]). En l'absence de toute notification dans ce délai, les autorités compétentes seront considérées par l'ABE comme ne s'y conformant pas. Les notifications doivent être transmises à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site internet de l'ABE et en indiquant en objet «EBA/GL/2019/02». Les notifications doivent être envoyées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes qu'elles représentent. Toute modification du statut de conformité avec les orientations doit également être signalée à l'ABE.

4. Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3.

[1] Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

2. Objet, champ d'application et définitions

Objet

5. Les présentes orientations précisent les dispositifs en matière de gouvernance interne, y compris en termes de gestion saine des risques, que les établissements, les établissements de paiement et les établissements de monnaie électronique doivent mettre en œuvre lorsqu'ils externalisent des fonctions, en particulier en ce qui concerne l'externalisation de fonctions critiques ou importantes.

6. Les orientations précisent comment les dispositifs visés au paragraphe précédent devraient être examinés et contrôlés par les autorités compétentes, au vu des dispositions de l'article 97 de la directive 2013/36/UE[2], du processus de contrôle et d'évaluation prudentiels («supervisory review and evaluation process» – SREP), de l'article 9, paragraphe 3, de la directive (UE) 2015/2366 [3], de l'article 5, paragraphe 5, de la directive 2009/110/CE [4], aux fins de l'accomplissement de leur obligation de contrôler le respect constant, par les entités destinataires des présentes orientations, des conditions de leur agrément.

Destinataires

7. Les présentes orientations sont destinées aux autorités compétentes au sens de l'article 4, paragraphe 1, point 40), du règlement (UE) n° 575/2013 [5], y compris la Banque centrale européenne en ce qui concerne les questions relatives aux missions que lui confie le règlement (UE) n° 1024/2013 [6], aux établissements au sens de l'article 4, paragraphe 1, point 3), du règlement (UE) n° 575/2013, aux établissements de paiement au sens de l'article 4, paragraphe 4, de la directive (UE) 2015/2366, et aux établissements de monnaie électronique au sens de l'article 2, paragraphe 1, de la directive 2009/110/UE. Les fournisseurs de services d'information sur les comptes fournissant uniquement le service visé à l'annexe I, point 8, de

[2] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.

[3] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

[4] Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE.

[5] Règlement (UE) nº 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 et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).

[6] Règlement (UE) nº 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit.

la directive (UE) 2015/2366 ne sont pas inclus dans le champ d'application des présentes orientations, conformément à l'article 33 de ladite directive.

8. Aux fins des présentes orientations, toute référence aux «établissements de paiement» inclut les «établissements de monnaie électronique» et toute référence aux «services de paiement» inclut l'«émission de monnaie électronique».

Champ d'application

9. Sans préjudice de la directive 2014/65/UE[7] et du règlement délégué (UE) 2017/565 de la Commission[8] (qui prévoit des obligations relatives à l'externalisation par les établissements qui fournissent des services d'investissement et exercent des activités d'investissement, de même que des lignes directrices établies par l'Autorité européenne des marchés financiers relatives aux services et activités d'investissement), les établissements au sens de l'article 3, paragraphe 1, point 3), de la directive 2013/36/UE doivent se conformer aux présentes orientations sur base individuelle, sous-consolidée et consolidée. L'application sur base individuelle peut faire l'objet d'une dispense par les autorités compétentes en vertu de l'article 21 de la directive 2013/36/UE ou de l'article 109, paragraphe 1, de la directive 2013/36/UE lu conjointement avec l'article 7 du règlement (UE) n° 575/2013. Les établissements relevant de la directive 2013/36/UE doivent se conformer à ladite directive et aux présentes orientations sur base consolidée et sous-consolidée comme prévu à l'article 21 et aux articles 108 à 110 de la directive 2013/36/UE.

10. Sans préjudice de l'article 8, paragraphe 3, de la directive (UE) 2015/2366 et de l'article 5, paragraphe 7, de la directive 2009/110/CE, les établissements de paiement et les établissements de monnaie électronique doivent se conformer aux présentes orientations sur base individuelle.

11. Les autorités compétentes responsables de la surveillance des établissements, des établissements de paiement et des établissements de monnaie électronique doivent se conformer aux présentes orientations.

Définitions

12. Sauf indication contraire, les termes utilisés et définis dans la directive 2013/36/UE, dans le règlement (UE) nº 575/2013, dans la directive 2009/110/UE, dans la directive (UE) 2015/2366 et dans les orientations de l'ABE sur la gouvernance interne[9] ont la même signification dans les présentes orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

[7] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

[8] Règlement délégué (UE) 2017/565 de la Commission du 25 avril 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles et les conditions d'exercice applicables aux entreprises d'investissement et la définition de certains termes aux fins de ladite directive (JO L 87 du 31.3.2017, p. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

Externalisation	accord, de quelque forme que ce soit, conclu entre un établissement, un établissement de paiement ou un établissement de monnaie électronique 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'établissement, l'établissement de paiement ou l'établissement de monnaie électronique lui-même.
Fonction	tous processus, services ou activités.
Fonction critique ou importante[10]	toute fonction considérée comme fonction critique ou importante comme énoncé à la section 4 des présentes orientations.
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[11].
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 externalisés.
Services en nuage	services fournis au moyen de l'informatique en nuage, à savoir un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (réseaux, serveurs, stockage, applications et services par exemple) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort ou d'intervention d'un prestataire de services.
Nuage public	infrastructure en nuage accessible au grand public en vue d'une utilisation ouverte.
Nuage privé	infrastructure en nuage accessible à un seul établissement ou établissement de paiement en vue d'une utilisation exclusive.
Nuage communautaire	infrastructure en nuage accessible à une communauté d'établissements ou d'établissements de paiement précise, y compris à plusieurs établissements d'un même groupe, en vue d'une utilisation exclusive.

[10] La formulation «fonction critique ou importante» se fonde sur la formulation utilisée dans la directive 2014/65/UE (MiFID II) et le règlement délégué (UE) 2017/565 complétant la directive MiFID II et n'est utilisée qu'en ce qui concerne l'externalisation; elle n'est pas liée à la définition des «fonctions critiques» en ce qui concerne le cadre pour le redressement et la résolution au sens de l'article 2, paragraphe 1, point 35, de la directive 2014/59/UE (DRRB).

[11] Les dispositions de la section 3 trouvent à s'appliquer à l'évaluation; d'autres documents de l'ABE désignent la sous-externalisation par les termes «chaîne d'externalisation» ou «externalisation en chaîne».

Nuage hybride	infrastructure en nuage composée d'au moins deux infrastructures en nuage distinctes.
Organe de direction	l'organe ou les organes d'un établissement ou d'un établissement de paiement, qui sont désignés conformément au droit national, qui sont compétents pour définir la stratégie, les objectifs et la direction globale de l'établissement ou de l'établissement de paiement 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'établissement ou de l'établissement de paiement et les administrateurs et personnes responsables de la direction de l'établissement de paiement.

3. Mise en œuvre

Date d'entrée en vigueur

13. À l'exception du paragraphe 63 (b), les présentes orientations s'appliquent à compter du 30 septembre 2019 à tous les accords d'externalisation conclus, révisés ou modifiés à partir de cette date. Le paragraphe 63 (b) s'applique à compter du 31 décembre 2021.

14. Les établissements et les établissements de paiement doivent examiner et modifier en conséquence tous les accords d'externalisation existants afin de garantir que ceux-ci sont en conformité avec les présentes orientations.

15. Dans les cas où la révision d'accords d'externalisation de fonctions essentielles ou importantes n'est pas finalisée au 31 décembre 2021, les établissements et les établissements de paiement doivent en informer leur autorité compétente en indiquant les mesures prévues pour conclure l'examen ou l'éventuelle stratégie de retrait.

Dispositions transitoires

16. Les établissements et les établissements de paiement doivent compléter la documentation de tous les accords d'externalisation existants, à l'exception des accords d'externalisation vers des fournisseurs de services en nuage, conformément aux présentes orientations, après la première date de renouvellement de chaque accord d'externalisation existant, mais au plus tard au 31 décembre 2021.

Abrogation

17. Les lignes directrices du Comité européen des contrôleurs bancaires (CECB) du 14 décembre 2006 relatives à l'externalisation ainsi que les recommandations de l'ABE sur l'externalisation vers des fournisseurs de services en nuage[12] sont abrogées à compter du 30 septembre 2019.

[12] Recommandations sur l'externalisation vers des fournisseurs de services en nuage (EBA/REC/2017/03).

4. Orientations relatives à l'externalisation

Titre I – Proportionnalité: application à l'échelon du groupe et systèmes de protection institutionnels

1 Proportionnalité

18. Lorsqu'ils respectent les présentes orientations ou en surveillent le respect des présentes orientations, les établissements, les établissements de paiement et les autorités compétentes devraient tenir compte du principe de proportionnalité. Le principe de proportionnalité vise à garantir que les dispositifs de gouvernance, y compris ceux liés à l'externalisation, sont compatibles avec le profil de risque individuel, la nature et le modèle d'entreprise de l'établissement ou de l'établissement de paiement, ainsi que la portée et la complexité de leurs activités, afin que les objectifs des exigences réglementaires soient effectivement atteints.

19. Lorsqu'ils appliquent les exigences prévues par les présentes orientations, les établissements et les établissements de paiement devraient tenir compte de la complexité des fonctions externalisées, des risques découlant du dispositif d'externalisation, du caractère critique ou de l'importance de la fonction externalisée, ainsi que de l'incidence potentielle de l'externalisation sur la poursuite de leurs activités.

20. Lorsqu'ils appliquent le principe de proportionnalité, les établissements, les établissements de paiement[13] et les autorités compétentes devraient tenir compte des critères énoncés au titre I des orientations de l'ABE sur la gouvernance interne conformément à l'article 74, paragraphe 2, de la directive 2013/36/UE.

2 Externalisation par des groupes et des établissements qui sont membres d'un système de protection institutionnel

21. Conformément à l'article 109, paragraphe 2, de la directive 2013/36/UE, les présentes orientations devraient également s'appliquer sur une base sous-consolidée et consolidée,

[13] Les établissements de paiement devraient également se référer aux orientations de l'ABE dans le cadre de la DSP2 concernant les informations à fournir pour l'agrément des établissements de paiement et des établissements de monnaie électronique et pour l'enregistrement des prestataires de services d'information sur les comptes, qui sont disponibles sur le site Internet de l'ABE sous le lien suivant: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

compte tenu du périmètre prudentiel de consolidation[14]. À cette fin, les entreprises mères de l'UE ou l'entreprise mère dans un État membre devraient s'assurer de la cohérence, de la bonne intégration et de l'adéquation des dispositifs, processus et mécanismes de gouvernance interne de leurs filiales, y compris les établissements de paiement, en vue de l'application effective des présentes orientations à tous les niveaux pertinents.

22. Les établissements et les établissements de paiement, conformément au paragraphe 21, ainsi que les établissements qui, en tant que membres d'un système de protection institutionnel, ont recours à des dispositifs de gouvernance centralisés, devraient se conformer aux dispositions suivantes:

    a. lorsque ces établissements ou établissements de paiement ont conclu des accords d'externalisation avec des prestataires de services au sein du groupe ou du système de protection institutionnel [15], l'organe de direction de ces établissements ou établissements de paiement conserve, pour ces accords d'externalisation également, l'entière responsabilité de veiller au respect de toutes les exigences réglementaires et de l'application effective des présentes orientations;

    b. lorsque ces établissements ou établissements de paiement confient les tâches opérationnelles des fonctions de contrôle interne à un prestataire de services au sein du groupe ou du système de protection institutionnel, en vue du suivi et de l'audit des dispositifs d'externalisation, les établissements devraient veiller à ce que, pour ces dispositifs d'externalisation également, ces tâches opérationnelles soient effectivement exécutées, notamment par la réception des rapports appropriés.

23. Outre les dispositions du paragraphe 22, les établissements et les établissements de paiement faisant partie d'un groupe auquel aucune exemption n'a été accordée sur la base de l'article 109 de la directive 2013/36/UE et de l'article 7 du règlement (UE) nº 575/2013, les établissements qui sont un organe central ou qui sont affiliés de manière permanente à un organe central pour lequel aucune exemption n'a été accordée sur la base de l'article 21 de la directive 2013/36/UE, ou les établissements qui sont membres d'un système de protection institutionnel, devraient prendre en considération les éléments suivants:

    a. lorsque le suivi opérationnel de l'externalisation est centralisé (par ex. dans le cadre d'un accord-cadre pour le suivi des dispositifs d'externalisation), les établissements et les établissements de paiement devraient veiller à ce qu'un suivi indépendant du prestataire de services et une surveillance appropriée par chaque établissement ou établissement de paiement soient possibles au moins pour les fonctions critiques ou importantes externalisées, y compris en recevant, au moins annuellement et sur demande de la fonction de suivi centralisé, des rapports comprenant au moins un

[14] Veuillez vous référer à l'article 4, paragraphe 1, points 47 et 48, du règlement (UE) nº 575/2013 concernant le périmètre de consolidation.

[15] Conformément à l'article 113, paragraphe 7, du CRR, un système de protection institutionnel est un arrangement de responsabilité contractuel ou prévu par la loi qui protège les établissements qui sont membres du système et, en particulier, garantit leur liquidité et leur solvabilité pour éviter la faillite, le cas échéant.

résumé de l'évaluation des risques et du suivi des performances. En outre, les établissements et les établissements de paiement devraient recevoir de la fonction de suivi centralisé un résumé des rapports d'audit pertinents relatifs à l'externalisation critique ou importante et, sur demande, le rapport d'audit complet;

b. les établissements et les établissements de paiement devraient 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 portant notamment sur les risques juridiques, le respect des exigences réglementaires et l'incidence sur les niveaux de service, afin qu'ils puissent évaluer l'incidence de ces changements;

c. lorsque ces établissements et établissements de paiement au sein du groupe, les établissements affiliés à un organe central ou les établissements faisant partie d'un système de protection institutionnel s'appuient sur une évaluation centrale des dispositifs d'externalisation préalable à l'externalisation, comme prévu à la section 12, chaque établissement et établissement de paiement devrait 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;

d. lorsque le registre de tous les dispositifs d'externalisation existants, tels que prévus à la section 11, est établi et tenu à jour de manière centralisée au sein d'un groupe ou d'un système de protection institutionnel, les autorités compétentes et tous les établissements et établissements de paiement devraient pouvoir obtenir leur propre registre sans délai indu. Ce registre devrait inclure tous les dispositifs d'externalisation, y compris les accords d'externalisation conclus avec des prestataires de services au sein de ce groupe ou de ce système de protection institutionnel;

e. lorsque ces établissements et établissements de paiement s'appuient sur un plan de sortie pour une fonction critique ou importante qui a été établi au niveau du groupe, au sein du système de protection institutionnel ou par l'organe central, tous les établissements et établissements de paiement devraient recevoir un résumé du plan et s'assurer que celui-ci peut être effectivement exécuté.

24. Lorsque des exemptions ont été accordées conformément à l'article 21 de la directive 2013/36/UE ou à l'article 109, paragraphe 1, de la directive 2013/36/UE, lu conjointement avec l'article 7 du règlement (UE) 575/2013, les dispositions des présentes orientations devraient être appliquées par l'entreprise mère dans un État membre, pour elle-même et pour ses filiales, ou par l'organe central et ses filiales dans leur ensemble.

25. Les établissements et les établissements de paiement qui sont des filiales d'une entreprise mère de l'UE ou d'une entreprise mère dans un État membre à laquelle aucune exemption n'a

été accordée sur la base de l'article 21 de la directive 2013/36/UE ou de l'article 109, paragraphe 1, de la directive 2013/36/UE, lu conjointement avec l'article 7 du règlement (UE) nº 575/2013, devraient veiller à respecter les présentes orientations sur base individuelle.

Titre II – Évaluation des dispositifs d'externalisation

3 Externalisation

26. Les établissements et les établissements de paiement devraient déterminer si un arrangement 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) relève normalement de fonctions qui seraient ou pourraient raisonnablement être exercées par des établissements ou des établissements de paiement, même si l'établissement ou l'établissement de paiement n'a pas lui-même exercé cette fonction par le passé.

27. Lorsqu'un accord conclu avec un prestataire de services couvre plusieurs fonctions, les établissements et les établissements de paiement devraient 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 devraient être examinés ensemble.

28. En règle générale, les établissements et les établissements de paiement ne devraient pas considérer les éléments suivants comme relevant de l'externalisation:

    a. une fonction qui doit obligatoirement être exercée par un prestataire de services, par ex. le contrôle légal des comptes;

    b. les services d'information de marché (par ex. la fourniture de données par Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. les infrastructures de réseaux mondiaux (par 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'établissement ou l'établissement de paiement (par ex. conseils d'un architecte, conseils juridiques et

représentation devant les tribunaux et les organes administratifs, nettoyage, jardinage et entretien des locaux de l'établissement ou de l'établissement de paiement, 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, lecteurs de cartes, fournitures de bureau, ordinateurs personnels, meubles) ou les services d'équipement (p. ex. électricité, gaz, eau, ligne téléphonique).

4 Fonctions critiques ou importantes

29. Les établissements et les établissements de paiement devraient toujours considérer une fonction comme critique ou importante dans les situations suivantes:[16]

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

        i. à la capacité des établissements de se conformer de manière continue aux conditions de leur agrément ou à leurs autres obligations au titre de la directive 2013/36/UE, du règlement (UE) nº 575/2013, de la directive 2014/65/UE, de la directive (UE) 2015/2366 et de la directive 2009/110/CE, ainsi qu'à leurs obligations réglementaires;

        ii. à leurs performances financières; ou

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

    b. lorsque les tâches opérationnelles des fonctions de contrôle interne sont externalisées, à moins que l'évaluation 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 l'efficacité de la fonction de contrôle interne;

    c. lorsqu'ils ont l'intention d'externaliser des fonctions d'activités bancaires ou de services de paiement dans une mesure qui nécessiterait l'autorisation[17] d'une autorité compétente, comme indiqué à la section 12.1.

30. Dans le cas des établissements, une attention particulière devrait 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 telles que définies à

[16] Voir également l'article 30 du règlement délégué (UE) 2017/565 de la Commission du 25 avril 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles et les conditions d'exercice applicables aux entreprises d'investissement et la définition de certains termes aux fins de ladite directive.

[17] Voir les activités énumérées à l'annexe I de la directive 2013/36/UE.

l'article 2, paragraphe 1, points 35 et 36, de la directive 2014/59/UE[18] et identifiées par les établissements selon les critères énoncés aux articles 6 et 7 du règlement délégué (UE) 2016/778 de la Commission.[19] Les fonctions nécessaires à l'exécution d'activités fondamentales ou de fonctions critiques devraient être considérées comme des fonctions critiques ou importantes aux fins des présentes orientations, à moins que l'évaluation de l'établissement 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.

31. Lorsqu'ils évaluent si un dispositif d'externalisation se rapporte à une fonction critique ou importante, les établissements et les établissements de paiement devraient tenir compte, outre des résultats de l'évaluation des risques énoncée à la section 12.2, au moins des facteurs suivants:

    a. si le dispositif d'externalisation est directement lié à la fourniture d'activités bancaires ou de services de paiement[20] pour lesquels ils sont agréés;

    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 technologies de l'information et de la communication (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;

[18] Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement et modifiant la directive 82/891/CEE du Conseil ainsi que les directives du Parlement européen et du Conseil 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE et 2013/36/UE et les règlements du Parlement européen et du Conseil (UE) nº 1093/2010 et (UE) nº 648/2012 (directive BRRD) (JO L 173 du 12.6.2014, p. 190).

[19] Règlement délégué (UE) nº 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 (JO L 131 du 20.5.2016, p. 41).

[20] Voir les activités énumérées à l'annexe I de la directive 2013/36/UE.

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

   i. à identifier, suivre 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'établissement ou de l'établissement de paiement 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'établissement ou l'établissement de paiement, 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'établissement ou l'établissement de paiement et ses clients, notamment, mais non exclusivement, le respect du règlement (UE) 2016/679[21].

[21] 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).

Titre III – Cadre de gouvernance

5 Dispositifs de bonne gouvernance et risque de tiers

32. Dans le cadre du dispositif de contrôle interne d'ensemble,[22] y compris les mécanismes de contrôle interne,[23] les établissements et les établissements de paiement devraient disposer d'un cadre global de gestion des risques à l'échelle de l'établissement, s'étendant à toutes les activités et unités internes. Dans ce cadre, les établissements et les établissements de paiement devraient identifier et gérer tous les risques auxquels ils sont exposés, y compris les risques résultant d'arrangements avec des tiers. Le cadre de la gestion des risques devrait également permettre aux établissements et aux établissements de paiement 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.[24]

33. Les établissements et les établissements de paiement, compte tenu du principe de proportionnalité et conformément à la section 1, devraient identifier, évaluer, surveiller et gérer tous les risques auxquels ils 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, y compris ceux visés aux paragraphes 26 et 28, devraient être évalués conformément à la section 12.2.

34. Les établissements et les établissements de paiement devraient veiller à se conformer à toutes les exigences du règlement (UE) 2016/679, y compris en ce qui concerne les arrangements conclus avec des tiers et les accords d'externalisation.

6 Des dispositifs de gouvernance et d'externalisation sains

35. L'externalisation de fonctions ne saurait entraîner la délégation des responsabilités de l'organe de direction. Les établissements et les établissements de paiement demeurent entièrement responsables du respect de toutes leurs obligations réglementaires, y compris leur capacité à surveiller l'externalisation de fonctions critiques ou importantes.

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

    a. s'assurer que l'établissement ou l'établissement de paiement satisfait en permanence aux conditions qu'il doit remplir pour rester agréé, y compris aux conditions imposées par l'autorité compétente, le cas échéant;

---

[22] Les établissements devraient se référer au titre V des orientations de l'ABE sur la gouvernance interne.

[23] Voir également l'article 11 de la directive 2015/2366 (DSP2).

[24] Voir également les orientations de l'ABE sur les TIC et la gestion des risques de sécurité (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) et les éléments fondamentaux du G7 pour la gestion des cyber-risques par des tiers dans le secteur financier (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

b. l'organisation interne de l'établissement ou de l'établissement de paiement;

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

d. la définition des stratégies et des politiques de l'établissement ou de l'établissement de paiement (par 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'établissement ou de l'établissement de paiement, 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.

37. L'externalisation ne devrait pas abaisser les exigences en matière d'adéquation d'aptitudes applicables aux membres de l'organe de direction d'un établissement, aux administrateurs et aux personnes responsables de la gestion de l'établissement de paiement, ainsi qu'aux responsables de fonctions clés. Les établissements et les établissements de paiement devraient 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.

38. Les établissements et les établissements de paiement devraient:

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

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

c. compte tenu de la section 1 des présentes orientations, établir une fonction d'externalisation ou désigner un cadre supérieur rendant compte directement à l'organe de direction (par ex. un reponsable 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 établissements, ainsi que de superviser la documentation des dispositifs d'externalisation. Les établissements ou les établissements de paiement de petite taille et moins complexes devraient au moins assurer une répartition claire 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'établissement ou de l'établissement de paiement.

39. Les établissements et les établissements de paiement devraient conserver en permanence une structure suffisante et ne pas devenir des «coquilles vides» ou des «sociétés boîtes aux lettres». À cette fin, ils devraient:

a. satisfaire en permanence à toutes les conditions de leur agrément [25], y compris l'exercice effectif par l'organe de direction de ses responsabilités telles que définies au paragraphe 36 des présentes orientations;

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

c. lorsque les tâches opérationnelles des fonctions de contrôle interne sont externalisées (par ex. en cas d'externalisation intragroupe ou d'externalisation dans le cadre de systèmes de protection institutionnels), exercer un contrôle approprié et être en mesure de gérer les risques engendrés par l'externalisation de fonctions critiques ou importantes; et

d. disposer de ressources et de capacités suffisantes pour assurer le respect des points a) à c).

40. En cas d'externalisation, les établissements et les établissements de paiement devraient au moins veiller:

a. à ce qu'ils 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 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);

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;

[25] Voir également les normes techniques de réglementation (RTS) visées à l'article 8, paragraphe 2, de la directive 2013/36/UE concernant les informations à communiquer pour l'agrément des établissements de crédit et les normes techniques d'exécution (ITS) visées à l'article 8, paragraphe 3, de la directive 2013/36/UE concernant les formulaires, modèles et procédures normalisés à utiliser pour la communication des informations nécessaires pour l'agrément des établissements de crédit (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Pour les établissements de paiement, veuillez vous référer aux orientations de l'ABE en vertu de la directive (UE) 2015/2366 (DSP2) sur les informations à communiquer pour l'agrément des établissements de paiement et des établissements de monnaie électronique et pour l'enregistrement des prestataires de services d'information sur les comptes (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

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'UE 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 règlement (UE) 2016/679.

7 Politique d'externalisation

41. L'organe de direction d'un établissement ou d'un établissement de paiement[26] qui a mis en place des dispositifs d'externalisation ou qui envisage de mettre en œuvre de tels dispositifs devrait 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, la politique d'externalisation devrait être conforme à la section 8 des orientations de l'ABE sur la gouvernance interne et, en particulier, devrait tenir compte des exigences énoncées à la section 18 (nouveaux produits et changements significatifs) de ces orientations. Les établissements de paiement peuvent également aligner leurs politiques sur les sections 8 et 18 des orientations de l'ABE sur la gouvernance interne.

42. La politique devrait 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 devrait couvrir au moins:

   a. les responsabilités de l'organe de direction conformément au paragraphe 36, y compris sa participation, le cas échéant, à la prise de décisions concernant l'externalisation de fonctions critiques ou importantes;

   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:

[26] Voir également les orientations de l'ABE sur les mesures de sécurité pour les risques opérationnels et de sécurité liés aux services de paiement dans le cadre de la DSP2, disponibles à l'adresse suivante: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

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

ii. les critères, y compris ceux mentionnés à la section 4, et les processus d'identification des fonctions critiques ou importantes;

iii. l'identification, l'évaluation et la gestion des risques conformément à la section 12.2;

iv. les vérifications nécessaires à l'égard des prestataires de services potentiels, y compris les mesures exigées en vertu de la section 12.3;

v. les procédures d'identification, d'évaluation, de gestion et d'atténuation des conflits d'intérêts potentiels, conformément à la section 8;

vi. la planification de la poursuite de l'activité conformément à la section 9;

vii. le processus d'approbation des nouveaux dispositifs d'externalisation;

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 à la section 14;

ii. les procédures de notification et de réaction aux changements liés à un dispositif d'externalisation ou à un prestataire de services (par 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. les processus de renouvellement;

e. les documents et la conservation d'informations, en tenant compte des exigences énoncées à la section 11;

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.

43. La politique d'externalisation devrait 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 et l'externalisation à ceux qui ne le sont pas;

c. les dispositifs d'externalisation intragroupe, les dispositifs d'externalisation au sein du même système de protection institutionnel (y compris les entités détenues individuellement ou collectivement à 100 % par des établissements relevant du système de protection institutionnel) 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.

44. Les établissements et les établissements de paiement devraient veiller à ce que la politique recense les effets potentiels suivants des dispositifs d'externalisations critiques ou importantes et à ce que ceux-ci soient pris en compte dans le processus décisionnel:

a. le profil de risque de l'établissement;

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.

8 Conflits d'intérêts

45. Les établissements, conformément au titre IV, section 11, des orientations de l'ABE sur la gouvernance interne,[27] et les établissements de paiement devraient identifier, évaluer et gérer les conflits d'intérêts liés à leurs dispositifs d'externalisation.

46. Lorsque l'externalisation donne lieu à des conflits d'intérêts importants, y compris entre entités du même groupe ou du même système de protection institutionnel, les établissements et les établissements de paiement doivent prendre les mesures appropriées pour gérer ces conflits d'intérêts.

47. Lorsque les fonctions sont assurées par un prestataire de services faisant partie d'un groupe ou d'un système de protection institutionnel ou est détenu par l'établissement, l'établissement de paiement, un groupe ou des établissements membres d'un système de protection institutionnel, les conditions, y compris les conditions financières, du service externalisé devraient 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 établissements au sein d'un groupe ou d'un système de protection institutionnel peuvent être prises en compte, pour autant que le prestataire de services reste

[27] Les établissements de paiement peuvent également aligner leurs politiques sur ces orientations.

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

9 Plans de poursuite de l'activité

48. Les établissements, conformément aux exigences de l'article 85, paragraphe 2, de la directive 2013/36/UE et du titre VI des orientations de l'ABE sur la gouvernance interne,[28] et les établissements de paiement devraient mettre en place, maintenir et tester périodiquement des plans appropriés de poursuite de l'activité pour les fonctions critiques ou importantes externalisées. Les établissements et les établissements de paiement faisant partie d'un groupe ou d'un système de protection institutionnel peuvent s'appuyer sur des plans de poursuite de l'activité établis de manière centralisée concernant leurs fonctions externalisées.

49. Les plans de poursuite de l'activité devraient 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 devraient 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.

[28] Disponible à l'adresse suivante: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

10 Fonction d'audit interne

50. Les activités de la fonction d'audit interne[29] devraient couvrir, selon une approche par les risques, l'examen indépendant des activités externalisées. Le plan[30] et le programme d'audit devraient comprendre, en particulier,la révision des dispositifs d'externalisation de fonctions critiques ou importantes.

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

    a. que le cadre d'externalisation de l'établissement ou de l'établissement de paiement, y compris la politique d'externalisation, est correctement et 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'établissement 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.

11 Exigences en matière de documentation

52. Dans le cadre de leur dispositif de gestion des risques, les établissements et les établissements de paiement devraient tenir à jour un registre comprenant des informations sur tous les dispositifs d'externalisation au sein de l'établissement et, le cas échéant, aux niveaux sous-consolidé et consolidé, comme indiqué à la section 2, et devraient 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. Compte tenu du droit national, les établissements devraient conserver la documentation relative à des accords d'externalisation résiliés ou arrivés à échéance dans le registre ainsi que les pièces justificatives pendant une durée appropriée.

---

[29] En ce qui concerne les responsabilités de la fonction d'audit interne, les établissements devraient se référer à la section 22 des orientations de l'ABE sur la gouvernance interne (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) et les établissements de paiement devraient se référer à l'orientation 5 des orientations de l'ABE sur l'agrément des établissements de paiement (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Voir également les orientations de l'ABE sur le processus de contrôle et d'évaluation prudentiels: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

53. Compte tenu du titre I des présentes orientations et dans les conditions prévues au paragraphe 23, point d), pour les établissements et les établissements de paiement au sein d'un groupe, les établissements affiliés de manière permanente à un organisme central ou les établissements qui sont membres du même système de protection institutionnel, le registre peut être tenu de manière centralisée.

54. Le registre devrait 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'établissement ou l'établissement de paiement;

    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 (par 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'établissement ou l'établissement de paiement qui reflète la nature de la fonction visée au point c) (par ex., technologie de l'information (TI), fonction de contrôle), ce qui devrait 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;

    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 nuage 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 devrait comprendre au moins les informations complémentaires suivantes:

a. les établissements, les établissements de paiement et autres entreprises inclus dans le périmètre de consolidation prudentielle ou, le cas échéant, dans le système de protection institutionnel, qui ont recours à l'externalisation;

b. si le prestataire de services ou le prestataire de services sous-traitant fait ou non partie du groupe ou est membre du système de protection institutionnel, s'il appartient à des établissements ou des établissements de paiement du groupe ou s'il est détenu par des membres d'un système de protection institutionnel;

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 (par ex. l'organe de direction) de l'établissement ou de l'établissement de paiement 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 de n^{ième} rang auxquels des parties significatives d'une fonction critique ou importante sont sous-externalisées, y compris le pays où les sous-traitants de n^{ième} rang 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'établissement ou l'établissement de paiement, 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.

56. Les établissements et les établissements de paiement devraient mettre à la disposition de l'autorité compétente, à sa demande, soit le registre complet de tous les dispositifs d'externalisation existants [31], 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 paragraphe 54, point d), des présentes orientations (par ex. tous les dispositifs d'externalisation informatique). Les établissements et les établissements de paiement

[31] Veuillez également consulter les orientations de l'ABE sur le processus de contrôle et d'évaluation prudentiels, disponibles à l'adresse suivante: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

devraient fournir ces informations sous une forme exploitable par ordinateur (par ex. un format de base de données couramment utilisé, des valeurs séparées par des virgules).

57. Les établissements et les établissements de paiement devraient mettre à la disposition de l'autorité compétente, à sa demande, toutes les informations nécessaires pour lui permettre d'assurer la surveillance effective de l'établissement ou de l'établissement de paiement, y compris, si nécessaire, une copie de l'accord d'externalisation.

58. Les établissements, sans préjudice de l'article 19, paragraphe 6, de la directive (UE) 2015/2366, et les établissements de paiement, devraient informer les autorités compétentes de manière adéquate et en temps utile, ou engager un dialogue prudentiel avec les autorités compétentes au sujet de l'externalisation envisagée de fonctions critiques ou importantes, et/ou lorsqu'une fonction externalisée est devenue critique ou importante, et elles devraient au moins fournir les informations visées au paragraphe 54.

59. Les établissements et les établissements de paiement[32] devraient informer en temps utile les autorités compétentes des changements significatifs et/ou des événements graves concernant leurs dispositifs d'externalisation qui pourraient avoir une incidence significative sur la poursuite des activités commerciales des établissements ou des établissements de paiement.

60. Les établissements et les établissements de paiement devraient documenter de manière appropriée les évaluations effectuées en application du titre IV et les résultats de leur suivi continu (par 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).

Titre IV – Processus d'externalisation

12 Analyse préalable à l'externalisation

61. Avant de conclure un accord d'externalisation, les établissements et les établissements de paiement devraient:

    a. évaluer si le dispositif d'externalisation concerne une fonction critique ou importante, telle que définie au titre II;

    b. évaluer si les conditions de surveillance de l'externalisation énoncées à la section 12.1 sont remplies;

    c. identifier et évaluer tous les risques pertinents du dispositif d'externalisation conformément à la section 12.2;

[32] Voir également les orientations de l'ABE sur la notification des incidents majeurs dans le cadre de la DSP2, disponibles à l'adresse suivante: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

d. effectuer les vérifications nécessaires à l'égard du prestataire de services potentiel, conformément à la section 12.3;

e. identifier et évaluer les conflits d'intérêts que l'externalisation pourrait entraîner conformément à la section 8.

12.1 Conditions de surveillance de l'externalisation

62. Les établissements et les établissements de paiement devraient veiller à ce que l'externalisation de fonctions d'activités bancaires[33] ou de services de paiement à un prestataire de services situé dans le même État membre ou dans un autre État membre, dans la mesure où l'exécution de cette fonction nécessite un agrément ou un enregistrement par une autorité compétente de l'État membre dans lequel ils sont agréés, ne soit effectuée que si l'une des conditions suivantes est remplie:

    a. le prestataire de services est agréé ou enregistré par une autorité compétente pour exercer ces activités bancaires ou ces services de paiement; ou

    b. le prestataire de services est par ailleurs autorisé à exercer ces activités bancaires ou ces services de paiement conformément au cadre juridique national applicable.

63. Les établissements et les établissements de paiement devraient veiller à ce que l'externalisation de fonctions d'activités bancaires ou de services de paiement à un prestataire de services situé dans un pays tiers, dans la mesure où l'exercice de cette fonction nécessite un agrément ou un enregistrement par une autorité compétente de l'État membre dans lequel ils sont agréés, ne soit effectuée 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»);

    b. il existe un accord de coopération approprié, par ex. sous la forme d'un protocole d'accord ou d'un accord de coordination organisant un collège de supervision, entre les autorités compétentes chargées de la surveillance de l'établissement et les autorités de surveillance chargées de la surveillance du prestataire de services; et

    c. l'accord de coopération visé au point b) devrait garantir que les autorités compétentes sont au moins en mesure:

        i. d'obtenir, sur demande, les informations nécessaires à l'accomplissement de leurs missions de surveillance conformément à la directive 2013/36/UE, au

[33] Voir l'article 9 du CRD en ce qui concerne l'interdiction faite 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.

règlement (UE) nº 575/2013, à la directive (UE) 2015/2366 ainsi qu'à la directive 2009/110/CE;

ii. d'obtenir un accès approprié aux données, documents, locaux ou personnel du pays tiers qui sont pertinents pour l'exercice de leurs pouvoirs de surveillance;

iii. de recevoir, dès que possible, des informations de l'autorité de surveillance du pays tiers pour enquêter sur des manquements manifestes aux exigences de la directive 2013/36/UE, du règlement (UE) nº 575/2013, de la directive (UE) 2015/2366 ainsi que de la directive 2009/110/CE; et

iv. de coopérer avec les autorités de surveillance compétentes du pays tiers en ce qui concerne l'application de la législation en cas de manquement aux exigences réglementaires applicables et de violation de la législation nationale de l'État membre. La coopération devrait inclure, sans nécessairement s'y limiter, la réception, dès que possible, d'informations sur les éventuels manquements aux exigences réglementaires applicables de la part des autorités de surveillance du pays tiers.

12.2 Évaluation des risques liés aux dispositifs d'externalisation

64. Les établissements et les établissements de paiement devraient évaluer l'incidence potentielle des dispositifs d'externalisation sur leurs risques opérationnels, tenir compte des résultats de l'évaluation lorsqu'ils décident si la fonction devrait 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.

65. L'évaluation devrait inclure, le cas échéant, des scénarios d'événements de risque potentiel, y compris des événements de risque opérationnel très élevé. Dans le cadre de l'analyse de scénarios, les établissements et les établissements de paiement devraient évaluer l'impact potentiel de services défaillants ou inadéquats, y compris les risques causés par les processus, systèmes, personnes ou événements externes. Les établissements et les établissements de paiement, compte tenu du principe de proportionnalité visé à la section 1, devraient documenter l'analyse effectuée et ses résultats et estimer dans quelle mesure le dispositif d'externalisation augmenterait ou réduirait leur risque opérationnel. Compte tenu du titre I, les établissements et les établissements de paiement de petite taille et non complexes peuvent utiliser des approches qualitatives d'évaluation des risques, tandis que les établissements de grande taille ou complexes devraient 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.

66. Dans le cadre de l'évaluation des risques, les établissements et les établissements de paiement devraient 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'établissement ou de l'établissement de paiement et, dans le cas de groupes d'établissements ou de systèmes de protection institutionnels, les risques agrégés sur une base consolidée ou sur la base du système de protection institutionnel;

c. dans le cas d'établissements importants, 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'établissement ou l'établissement de paiement et par le prestataire de services pour gérer et atténuer les risques.

67. Lorsque le dispositif d'externalisation prévoit la possibilité que le prestataire de services sous-traite des fonctions critiques ou importantes à d'autres prestataires de services, les établissements et les établissements de paiement devraient tenir compte:

a. des risques associés à la sous-externalisation, y compris les risques supplémentaires qui peuvent survenir si le sous-traitant de n^{ième} rang 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 établissements ou des établissements de paiement à contrôler la fonction critique ou importante externalisée et la capacité des autorités compétentes à les surveiller efficacement.

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 établissements et les établissements de paiement devraient, au moins:

a. identifier et classifier les fonctions pertinentes et les données et systèmes connexes au regard de leur sensibilité 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, et 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'UE);

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 de la loi sur l'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'établissement ou de l'établissement de paiement 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 établissements et les établissements de paiement devraient 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'établissement, s'il est inclus dans le périmètre de consolidation comptable ou s'il est membre, ou appartient à des établissements qui sont membres, d'un système de protection institutionnel et, si tel est le cas, la mesure dans laquelle l'établissement contrôle le prestataire de services ou peut exercer une influence sur ses actions conformément à la section 2.

12.3 Diligence appropriée

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

70. En ce qui concerne les fonctions critiques et importantes, les établissements et les établissements de paiement devraient 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, informatiques, financières), la structure organisationnelle et, le cas échéant, l'(les) agrément(s) ou l'(les) enregistrement(s) réglementaire(s) nécessaire(s) pour exercer la fonction critique ou importante de manière fiable et professionnelle, de façon à satisfaire à ses obligations pendant toute la durée du projet de contrat.

71. 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'établissement ou de l'établissement de paiement;

    c. si le prestataire de services est l'entreprise mère ou une filiale de l'établissement ou de l'établissement de paiement, s'il fait partie du périmètre comptable de consolidation de l'établissement ou s'il est membre, ou appartient à des établissements qui sont membres, du système de protection institutionnel auquel l'établissement appartient;

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

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

73. Les établissements et les établissements de paiement devraient 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 établissements et les établissements de paiement devraient 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 (par 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.

13 Phase contractuelle

74. Les droits et obligations de l'établissement, de l'établissement de paiement et du prestataire de services devraient être clairement répartis et définis dans un accord écrit.

75. L'accord d'externalisation de fonctions critiques ou importantes devrait au moins 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'établissement ou l'établissement de paiement;

c. la législation applicable à l'accord;

d. les obligations financières des parties;

e. si la sous-externalisation d'une fonction critique ou importante, ou de parties significatives de celle-ci, est autorisée ou non et, dans l'affirmative, les conditions énoncées à la section 13.1 qui sont applicables à la sous-externalisation;

f. le(s) lieu(x) (c.-à-d. les régions ou pays) où la fonction critique ou importante 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'établissement ou l'établissement de paiement 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 à la section 13.2;

h. le droit de l'établissement ou de l'établissement de paiement de contrôler en permanence les performances du prestataire de services;

i. les niveaux de service convenus, qui devraient 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'établissement ou l'établissement de paiement, 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 critique ou importante selon les niveaux de service convenus et conformément aux lois et aux exigences réglementaires applicables 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 devrait 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 l'établissement ou l'établissement de paiement 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 les autorités de résolution de l'établissement ou de l'établissement de paiement, y compris avec les autres personnes désignées par celles-ci;

o. pour les établissements, une référence claire aux pouvoirs de l'autorité nationale de résolution, en particulier aux articles 68 et 71 de la directive 2014/59/UE (directive BRRD), et notamment une description des «obligations essentielles» du contrat au sens de l'article 68 de ladite directive;

p. le droit inconditionnel des établissements, des établissements de paiement et des autorités compétentes d'inspecter et d'auditer le prestataire de services en ce qui concerne, en particulier, la fonction critique ou importante externalisée, comme indiqué à la section 13.3;

q. les droits de résiliation, tels que précisés à la section 13.4.

13.1 Sous-externalisation de fonctions critiques ou importantes

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

77. Si la sous-externalisation de fonctions critiques ou importantes est autorisée, les établissements et les établissements de paiement devraient 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, ils devraient l'inscrire au registre.

78. Si la sous- externalisation de fonctions critiques ou importantes est permise, l'accord écrit devrait:

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'établissement ou l'établissement de paiement sont constamment respectées;

d. exiger du prestataire de services qu'il obtienne au préalable l'autorisation écrite, spécifique ou générale de l'établissement ou de l'établissement de paiement avant de sous-externaliser des données;[34]

e. prévoir l'obligation pour le prestataire de services d'informer l'établissement ou l'établissement de paiement 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 de n^{ième} rang et le délai de notification; en particulier, le délai de notification à fixer devrait permettre à l'établissement ou à l'établissement de paiement pratiquant l'externalisation 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'établissement ou l'établissement de paiement 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'établissement ou l'établissement de paiement 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'établissement ou l'établissement de paiement, ou lorsque le prestataire de services sous-externalise les services sans en informer l'établissement ou l'établissement de paiement.

79. Les établissements et les établissements de paiement ne devraient accepter la sous-externalisation que si le sous-traitant de nième rang s'engage:

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

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

80. Les établissements et les établissements de paiement devraient s'assurer que le prestataire de services contrôle de manière appropriée les prestataires de services sous-traitants de nième rang, conformément à la politique définie par l'établissement ou l'établissement de paiement. 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 paragraphe 79 ne sont pas

[34] Voir l'article 28 du règlement (UE) 2016/679.

remplies, l'établissement ou l'établissement de paiement devrait exercer son droit de s'opposer à la sous-externalisation, si ce droit a été convenu, et/ou de résilier le contrat.

13.2 Sécurité des données et systèmes

81. Les établissements et les établissements de paiement devraient veiller à ce que les prestataires de services, le cas échéant, respectent les normes de sécurité informatique appropriées.

82. Le cas échéant (p. ex. dans le contexte de l'externalisation de services en nuage ou d'autres services TIC), les établissements et les établissements de paiement devraient 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.

83. 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 établissements et les établissements de paiement devraient adopter une approche par 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) et les considérations relatives à la sécurité informatique.

84. Sans préjudice des exigences du règlement (UE) 2016/679, lorsqu'ils externalisent des services (en particulier vers des pays tiers), les établissements et les établissements de paiement devraient tenir compte des différences entre les dispositions nationales concernant la protection des données. Les établissements et les établissements de paiement devraient veiller à ce que l'accord d'externalisation prévoie 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'établissement ou à l'établissement de paiement (par 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).

13.3 Droits d'accès, d'information et d'audit

85. Les établissements et les établissements de paiement devraient s'assurer, dans le cadre de l'accord d'externalisation écrit, que la fonction d'audit interne est en mesure d'examiner la fonction externalisée selon une approche par les risques.

86. Indépendamment du caractère critique ou important de la fonction externalisée, les accords d'externalisation écrits conclus entre les établissements et les prestataires de services devraient faire référence aux pouvoirs de collecte d'informations et d'enquête des autorités compétentes et des autorités de résolution en vertu de l'article 63, paragraphe 1, point a), de la directive 2014/59/UE et de l'article 65, paragraphe 3, de la directive 2013/36/UE en ce qui concerne les prestataires de services situés dans un État membre, et devraient également garantir ces droits en ce qui concerne les prestataires de services situés dans des pays tiers.

87. En ce qui concerne l'externalisation de fonctions critiques ou importantes, les établissements et les établissements de paiement devraient veiller, dans l'accord d'externalisation écrit, à ce que le prestataire de services leur accorde, ainsi qu'à leurs autorités compétentes, y compris les autorités de résolution, et à toute autre personne désignée par eux ou par les autorités compétentes, 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»), afin de leur permettre de contrôler le dispositif d'externalisation et de s'assurer du respect de toutes les exigences réglementaires et contractuelles applicables.

88. En ce qui concerne l'externalisation de fonctions qui ne sont pas critiques ou importantes, les établissements et les établissements de paiement devraient garantir les droits d'accès et d'audit prévus au paragraphe 87, points a) et b), et à la section 13.3, selon une approche par 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 établissements et les établissements de paiement devraient tenir compte du fait que les fonctions peuvent devenir critiques ou importantes au fil du temps.

89. Les établissements et les établissements de paiement devraient 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 les établissements, par les autorités compétentes ou par les tiers désignés par eux pour exercer ces droits.

90. Les établissements et les établissements de paiement devraient exercer leurs droits d'accès et d'audit, déterminer la fréquence des audits et les domaines à auditer selon une approche par les risques et se conformer à des normes d'audit nationales et internationales pertinentes et communément acceptées.[35]

91. Sans préjudice de leur responsabilité finale en ce qui concerne les dispositifs d'externalisation, les établissements et les établissements de paiement 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

[35] Pour les établissements, veuillez vous référer à la section 22 des orientations de l'ABE sur la gouvernance interne: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

de réduire la charge organisationnelle tant pour les clients que pour le prestataire de services;

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

92. En ce qui concerne l'externalisation de fonctions critiques ou importantes, les établissements et les établissements de paiement devraient évaluer si les certifications et les rapports visés au paragraphe 91, point b), sont adéquats et suffisants pour se conformer à leurs obligations réglementaires et ne devraient pas se fier uniquement à ces rapports sur le long terme.

93. Les établissements et les établissements de paiement ne devraient recourir à la méthode visée au paragraphe 91, point b), que s'ils:

a. sont satisfaits 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'établissement ou l'établissement de paiement, 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 satisfaits 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, 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 devraient 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.

94. Conformément aux orientations de l'ABE sur l'évaluation des risques liés aux TIC dans le cadre du SREP, les établissements devraient, le cas échéant, s'assurer qu'ils 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.[36] Eu égard au titre I, les établissements de paiement devraient également disposer de mécanismes de contrôle des TIC internes, y compris des mesures de contrôle de la sécurité des TIC et des mesures d'atténuation.

95. Avant toute planification d'inspection sur place et dans un délai raisonnable, les établissements, les établissements de paiement, les autorités compétentes et les auditeurs, ou les tiers agissant au nom de l'établissement, de l'établissement de paiement ou des autorités compétentes devraient 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.

96. 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.

97. Lorsque le dispositif d'externalisation présente un niveau élevé de complexité technique, par exemple dans le cas de l'externalisation en nuage, l'établissement ou l'établissement de paiement devrait 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'établissement ou de l'établissement de paiement qui examine les certifications ou les audits effectués par les prestataires de services.

13.4 Droits de résiliation

98. Le dispositif d'externalisation devrait expressément prévoir la possibilité pour l'établissement ou l'établissement de paiement de résilier l'accord, conformément à la législation applicable, y compris dans les situations suivantes:

    a. lorsque le prestataire 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;

[36] Voir également les orientations de l'ABE sur les risques liés aux TIC: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

c. lorsqu'il se produit des changements significatifs concernant le dispositif d'externalisation ou le prestataire de services (par ex., sous-externalisation ou changement de sous-traitants de n^{ième} rang);

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'établissement ou de l'établissement de paiement, par exemple dans le cas où l'autorité compétente n'est plus en mesure de surveiller efficacement l'établissement ou l'établissement de paiement du fait du dispositif d'externalisation.

99. L'accord d'externalisation devrait faciliter le transfert de la fonction externalisée vers un autre prestataire de services ou la réinternalisation de la fonction dans l'établissement ou l'établissement de paiement. À cette fin, l'accord d'externalisation écrit devrait:

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'établissement ou à l'établissement de paiement, 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; et

c. prévoir l'obligation pour le prestataire de services d'aider l'établissement ou l'établissement de paiement à assurer le transfert ordonné de la fonction en cas de résiliation de l'accord d'externalisation.

14 Contrôle des fonctions externalisées

100. Les établissements et les établissements de paiement devraient effectuer le suivi permanent des performances des prestataires de services en ce qui concerne tous les dispositifs d'externalisation selon une approche par les risques, l'accent étant mis principalement sur l'externalisation de fonctions critiques ou importantes, en veillant notamment à garantir 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 établissements et les établissements de paiement devraient réévaluer le caractère critique ou important de cette fonction conformément à la section 4.

101. Les établissements et les établissements de paiement devraient faire preuve de la compétence, du soin et de la diligence nécessaires dans le suivi et la gestion des dispositifs d'externalisation.

102. Les établissements devraient régulièrement mettre à jour leur évaluation des risques conformément à la section 12.2 et informer périodiquement l'organe de direction des risques identifiés en ce qui concerne l'externalisation de fonctions critiques ou importantes.

103. Les établissements et les établissements de paiement devraient surveiller et gérer les risques internes de concentration auxquels ils sont confrontés en lien avec les dispositifs d'externalisation, compte tenu de la section 12.2 des présentes orientations.

104. Les établissements et les établissements de paiement devraient 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, ils devraient:

a. s'assurer qu'ils 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.

105. Les établissements devraient prendre des mesures appropriées s'ils constatent des lacunes dans l'exercice de la fonction externalisée. En particulier, les établissements et les établissements de paiement devraient 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 établissements et les établissements de paiement devraient 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.

15 Stratégies de sortie

106. Lorsqu'ils externalisent des fonctions critiques ou importantes, les établissements et les établissements de paiement devraient disposer d'une stratégie de sortie documentée qui soit conforme à leur politique d'externalisation ainsi qu'à leurs plans de continuité de l'activité[37], et qui prenne au moins en compte les éventualités suivantes:

a. la résiliation des accords d'externalisation;

[37] Conformément aux exigences de l'article 85, paragraphe 2, de la directive 2013/36/UE et du titre VI des orientations de l'ABE sur la gouvernance interne, les établissements et les établissements de paiement devraient disposer de plans appropriés de poursuite de l'activité en ce qui concerne l'externalisation de fonctions critiques ou importantes.

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.

107. Les établissements et les établissements de paiement devraient s'assurer qu'ils 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'ils fournissent aux clients. Pour ce faire, ils devraient:

a. élaborer et mettre en œuvre des plans de sortie complets, documentés et suffisamment testés, le cas échéant (par ex., en effectuant une analyse des 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'établissement ou à l'établissement de paiement 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.

108. Lors de l'élaboration de stratégies de sortie, les établissements et les établissements de paiement devraient:

a. définir les objectifs de la stratégie 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 à la section 14), y compris des indicateurs fondés sur des niveaux de service inacceptables qui devraient déclencher la sortie.

Titre V – Orientations relatives à l'externalisation à l'intention des autorités compétentes

109. Lorsqu'elles établissent des méthodes appropriées pour contrôler le respect par les établissements et les établissements de paiement des conditions de leur agrément initial, les autorités compétentes devraient s'efforcer de déterminer si les dispositifs d'externalisation constituent un changement significatif concernant les conditions et obligations de l'agrément initial des établissements et des établissements de paiement.

110. Les autorités compétentes devraient veiller à être en mesure de surveiller efficacement les établissements et les établissements de paiement et devraient notamment veiller à ce que les établissements ou les établissements de paiement se soient assurés, dans leur accord d'externalisation, que les prestataires de services sont tenus d'accorder des droits de contrôle et d'accès à l'autorité compétente et à l'établissement, conformément à la section 13.3.

111. L'analyse des risques liés à l'externalisation auxquels les établissements sont confrontés devrait être effectuée au moins au sein du SREP ou, en ce qui concerne les établissements de paiement, dans le cadre d'autres processus de surveillance, y compris des demandes ad hoc, ou lors d'inspections sur place.

112. Outre les informations inscrites au registre conformément à la section 11, les autorités compétentes peuvent demander aux établissements et aux établissements de paiement des informations complémentaires, notamment en ce qui concerne les dispositifs d'externalisation de fonctions critiques ou importantes, telles que:

a. l'analyse détaillée des risques;

b. si le prestataire de services dispose d'un plan de continuité de l'activité adapté aux services fournis à l'établissement ou à l'établissement de paiement pratiquant l'externalisation;

c. la stratégie de sortie à mettre en œuvre si l'accord d'externalisation est résilié par l'une ou l'autre des parties ou en cas de perturbations dans la fourniture des services; et

d. les ressources et les mesures mises en place pour contrôler adéquatement les activités externalisées.

113. Outre les informations exigées en vertu de la section 11, les autorités compétentes peuvent exiger des établissements et des établissements de paiement qu'ils fournissent des informations détaillées sur tout dispositif d'externalisation, même si la fonction concernée n'est pas considérée comme critique ou importante.

114. Les autorités compétentes devraient évaluer les éléments suivants selon une approche par les risques:

a. si les établissements et les établissements de paiement contrôlent et gèrent de manière appropriée, en particulier, les dispositifs d'externalisation critiques ou importants;

b. si les établissements et les établissements de paiement disposent de ressources suffisantes pour contrôler et gérer les dispositifs d'externalisation;

c. si les établissements et les établissements de paiement identifient et gèrent tous les risques pertinents; et

d. si les établissements et les établissements de paiement identifient, évaluent et gèrent de manière appropriée les conflits d'intérêts en ce qui concerne les dispositifs d'externalisation, par exemple en cas d'externalisation intragroupe ou au sein d'un même système de protection institutionnel.

115. Les autorités compétentes devraient veiller à ce que les établissements et les établissements de paiement de l'UE/EEE ne fonctionnent pas comme une «coquille vide», y compris lorsque les établissements utilisent des transactions adossées ou des transactions intragroupe pour transférer une partie du risque de marché et du risque de crédit à une entité hors UE/EEE, et elles devraient veiller à ce qu'ils mettent en place des dispositifs appropriés en matière de gouvernance et de gestion des risques pour identifier et gérer les risques auxquels ils sont exposés.

116. Dans leur évaluation, les autorités compétentes devraient tenir compte de tous les risques, en particulier:[38]

a. les risques[39] opérationnels liés au dispositif d'externalisation;

b. les risques de réputation;

c. le risque d'intervention *(«step-in risks»*)qui pourrait obliger l'établissement à renflouer un prestataire de services, dans le cas d'établissements importants;

d. les risques de concentration au sein de l'établissement, y compris sur une base consolidée, liés à des arrangements d'externalisation multiples conclus avec un même prestataire de services ou des prestataires de services étroitement liés, ou à des arrangements d'externalisation multiples au sein d'un même domaine d'activité;

[38] Pour les établissements soumis à la directive 2013/36/UE, voir également les orientations de l'ABE sur le SREP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Voir également les orientations de l'ABE sur les risques liés aux TIC: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

e. les risques de concentration au niveau sectoriel, par exemple lorsque plusieurs établissements ou établissements de paiement font appel à un même prestataire de services ou à un petit groupe de prestataires de services;

f. la mesure dans laquelle l'établissement ou l'établissement de paiement pratiquant l'externalisation contrôle le prestataire de services ou peut exercer une influence sur ses actions, la réduction des risques pouvant résulter d'un niveau de contrôle plus élevé, et si le prestataire de services relève du contrôle sur une base consolidée du groupe; et

g. les risques de conflits d'intérêts entre l'établissement et le prestataire de services.

117. Lorsque des risques de concentration sont identifiés, les autorités compétentes devraient contrôler l'évolution de ces risques et évaluer à la fois leur impact potentiel sur les autres établissements et établissements de paiement et la stabilité du marché financier; le cas échéant, les autorités compétentes devraient informer l'autorité de résolution des nouvelles fonctions potentiellement critiques[40] qui ont été identifiées au cours de cette évaluation.

118. Lorsque des préoccupations sont identifiées qui conduisent à conclure qu'un établissement ou un établissement de paiement ne dispose plus de dispositifs de gouvernance solides ou ne se conforme pas aux exigences réglementaires, les autorités compétentes devraient prendre des mesures appropriées, telles que la limitation ou la restriction du périmètre des fonctions externalisées ou l'obligation de se retirer d'un ou de plusieurs dispositifs d'externalisation. En particulier, compte tenu de la nécessité pour l'établissement ou l'établissement de paiement de fonctionner de manière continue, la résiliation de contrats pourrait être nécessaire si la surveillance et le respect des exigences réglementaires ne peuvent être garantis par d'autres mesures.

119. Les autorités compétentes devraient s'assurer qu'elles sont en mesure d'exercer une surveillance efficace, en particulier lorsque les établissements et les établissements de paiement externalisent des fonctions critiques ou importantes qui sont exercées en dehors de l'UE/EEE.

[40] Au sens de l'article 2, paragraphe 1, point 35, de la directive BRRD.