EBA/REC/2017/03

28/03/2018

Recommandations

sur l'externalisation vers des fournisseurs de services en nuage

1. Obligations de conformité et de déclaration

Statut de ces recommandations

1. Le présent document contient des recommandations émises conformément à l'article 16 du règlement (UE) n° 1093/2010[1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces recommandations.

2. Les recommandations 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) n° 1093/2010, qui sont soumises aux recommandations, devraient s'y conformer en les intégrant de manière appropriée dans leurs pratiques, (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les recommandations s'adressent principalement aux établissements financiers.

Exigences de notification

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes doivent notifier à l'ABE si elles respectent ou entendent respecter les présentes recommandations, ou communiquer, dans le cas contraire, les motifs de leur non-respect avant le 28/05/2018. En l'absence de notification dans ce délai, l'ABE considérera que les autorités compétentes ne respectent pas les recommandations. Les notifications sont à adresser à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site web de l'ABE, sous la référence «EBA/REC/2017/03». Les notifications doivent être soumises par des personnes disposant des pouvoirs nécessaires pour rendre compte de la conformité au nom des autorités compétentes. Toute modification du statut de conformité avec les recommandations doit être signalée à l'ABE.

4. Conformément à l'article 16, paragraphe 3, les notifications seront publiées sur le site web de l'ABE.

[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 et champ d'application

1. Les présentes recommandations précisent les conditions applicables à l'externalisation visée dans les orientations du CECB du 14 décembre 2006 relatives à l'externalisation et s'appliquent à l'externalisation par des établissements, au sens de l'article 4, paragraphe 1, point 3), du règlement (UE) nº 575/2013, vers des fournisseurs de services en nuage.

Destinataires

2. Les présentes recommandations sont destinées aux autorités compétentes, au sens de l'article 4, paragraphe 2, point i), du règlement (UE) nº 1093/2010 et aux établissements, au sens de l'article 4, paragraphe 1, point 3), du règlement (UE) nº 575/2013[2].

Définitions

3. Sauf indication contraire, les termes utilisés et définis dans la directive 2013/36/UE[3] relative aux exigences de fonds propres et dans les orientations du CECB revêtent la même signification dans ces recommandations. En outre, aux fins des présentes recommandations, les définitions suivantes s'appliquent:

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 en vue d'une utilisation exclusive.

[2] 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.

[3] 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.

Nuage communautaire	Infrastructure en nuage accessible à une communauté d'établissements précise, y compris à plusieurs établissements d'un même groupe, en vue d'une utilisation exclusive.
Nuage hybride	Infrastructure en nuage composée d'au moins deux infrastructures en nuage distinctes.

3. Mise en œuvre

Date d'entrée en vigueur

5. Les présentes recommandations s'appliquent à compter du 1er juillet 2018.

4. Recommandations sur l'externalisation vers des fournisseurs de services en nuage

4.1 Évaluation du caractère significatif

1. Avant toute externalisation de leurs activités, les établissements pratiquant l'externalisation devraient évaluer quelles activités devraient être considérées comme significatives. Ils devraient procéder à cette évaluation du caractère significatif des activités sur la base de l'orientation 1, point f), des orientations du CECB et, en ce qui concerne précisément l'externalisation vers des fournisseurs de services en nuage, en prenant en considération l'ensemble des éléments suivants:

    (a) le caractère critique des activités à externaliser et le profil de risque inhérent à ces dernières, c'est-à-dire déterminer si les activités sont critiques pour la viabilité/continuité d'activité de l'établissement et ses obligations envers ses clients;

    (b) l'incidence opérationnelle directe des interruptions de service, et les risques juridiques et de réputation connexes;

    (c) l'incidence que toute interruption de l'activité pourrait avoir sur les perspectives de revenus de l'établissement;

    (d) l'incidence potentielle qu'une violation de la confidentialité ou l'incapacité à assurer l'intégrité des données pourraient avoir sur l'établissement et sur ses clients.

4.2 Obligation d'informer les autorités de contrôle de manière adéquate

2. Les établissements pratiquant l'externalisation devraient communiquer de manière adéquate aux autorités compétentes les activités significatives à externaliser vers des fournisseurs de services en nuage, et ce sur la base du point 4.3 des orientations du CECB et, en tout état de cause, mettre les informations suivantes à la disposition de ces autorités:

    (a) le nom du fournisseur de services en nuage et le nom de sa société mère (s'il en a une);
    (b) une description des activités et des données à externaliser;
    (c) le(s) pays au sein duquel ou desquels le service sera exécuté (y compris la localisation des données);
    (d) la date de début du service;
    (e) la date du dernier renouvellement du contrat (le cas échéant);
    (f) la législation applicable régissant le contrat;

(g) la date d'expiration du service ou la prochaine date de renouvellement du contrat (le cas échéant).

3. Outre les informations fournies conformément au point précédent, l'autorité compétente peut demander à l'établissement pratiquant l'externalisation de fournir des informations complémentaires sur son analyse de risque relative aux activités significatives à externaliser, et notamment préciser si:

   (a) le fournisseur de services en nuage dispose d'un plan de continuité des activités adapté aux services fournis à l'établissement pratiquant l'externalisation;
   (b) l'établissement pratiquant l'externalisation dispose d'une stratégie de retrait en cas de résiliation par l'une des parties ou en cas d'interruption de la prestation de services par le fournisseur de services en nuage;
   (c) l'établissement pratiquant l'externalisation maintient les compétences et les ressources nécessaires au suivi adéquat des activités externalisées.

4. L'établissement pratiquant l'externalisation devrait tenir à jour un registre des informations sur l'ensemble de ses activités significatives et non significatives externalisées vers des fournisseurs de services en nuage à l'échelon de l'établissement et du groupe. L'établissement pratiquant l'externalisation devrait mettre à la disposition de l'autorité compétente, à sa demande, une copie de l'accord d'externalisation et des informations y afférentes consignées dans ce registre, que l'activité externalisée vers un fournisseur de services en nuage ait été ou non considérée comme significative par l'établissement.

5. Le registre visé au point précédent devrait inclure au minimum les informations suivantes:

   (a) les informations visées au point 2, de a) à g), si elles n'ont pas encore été fournies;
   (b) le type d'externalisation (le modèle de services en nuage et le modèle de déploiement en nuage, à savoir les nuages public/privé/hybride/communautaire);
   (c) les bénéficiaires des services en nuage en vertu de l'accord d'externalisation;
   (d) les preuves de l'autorisation d'externalisation par l'organe de direction ou par ses comités délégués, le cas échéant;
   (e) le nom des éventuels sous-traitants de nième rang, le cas échéant;
   (f) le pays d'enregistrement du fournisseur de services en nuage/du principal sous-traitant de second rang;
   (g) la confirmation (ou non), après évaluation, du caractère significatif de l'externalisation;
   (h) la date de la dernière évaluation du caractère significatif des activités externalisées de l'établissement;
   (i) la confirmation (ou non) que le fournisseur de services en nuage/le ou les sous-traitant(s) de nième rang soutiennent des opérations métier soumises à des exigences horaires pour leur fonctionnement;
   (j) une évaluation de la substituabilité (facile, difficile ou impossible) du fournisseur de services en nuage;
   (k) l'identité d'un fournisseur de services alternatif, lorsque cela est possible;

(l) la date de la dernière évaluation des risques relative à l'accord d'externalisation ou de sous-traitance de nième rang.

4.3 Droits d'accès et d'audit

En ce qui concerne les établissements

6. Sur la base de l'orientation 8, paragraphe 2, point g), des orientations du CECB et aux fins de l'externalisation en nuage, les établissements pratiquant l'externalisation devraient en outre veiller à disposer d'un accord écrit avec le fournisseur de services en nuage, par lequel ce dernier s'engage à:

   (a) fournir à l'établissement, à tout tiers désigné à cet effet par l'établissement et au contrôleur légal des comptes de l'établissement un accès complet à ses locaux professionnels (siège social et centres opérationnels), y compris à l'ensemble des dispositifs, systèmes, réseaux et données utilisés pour la fourniture des services externalisés (droit d'accès);

   (b) conférer à l'établissement, à tout tiers désigné à cet effet par l'établissement et au contrôleur légal des comptes de l'établissement, des droits illimités en matière d'inspection et d'audit des services externalisés (droit d'audit).

7. L'exercice effectif des droits d'accès et d'audit ne devrait pas être entravé ou limité par des arrangements contractuels. Si la réalisation d'audits ou l'utilisation de certaines méthodes d'audit sont susceptibles de poser un risque pour l'environnement d'un autre client, il convient de définir, d'un commun accord, d'autres manières de parvenir à un niveau d'assurance similaire à celui requis par l'établissement.

8. L'établissement pratiquant l'externalisation devrait exercer ses droits d'audit et d'accès en se fondant sur les risques. Si un établissement pratiquant l'externalisation n'utilise pas ses propres ressources d'audit, il devrait envisager de recourir à au moins l'un des outils suivants:

   (a) des audits regroupés organisés conjointement avec d'autres clients du même fournisseur de services en nuage, et réalisés par ces clients ou par un tiers désigné par eux, afin d'utiliser plus efficacement les ressources d'audit et de réduire la charge organisationnelle tant pour les clients que pour le fournisseur de services en nuage;

   (b) des certifications de tiers et des rapports d'audit interne ou de tiers mis à disposition par le fournisseur de services en nuage, à condition que:

      i. l'établissement pratiquant l'externalisation veille 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 cet établissement;
      ii. l'établissement pratiquant l'externalisation effectue régulièrement un examen minutieux du contenu des certifications ou des rapports d'audit, et s'assure en

particulier que les contrôles clés sont toujours couverts dans les futures versions des rapports d'audit et vérifie que la certification ou le rapport d'audit n'est pas obsolète;

iii. l'établissement pratiquant l'externalisation soit satisfait de l'aptitude de la partie chargée de la certification ou de l'audit (notamment en ce qui concerne la rotation de l'entreprise chargée de la certification ou de l'audit, les qualifications, l'expertise, la réexécution/vérification des éléments probants inclus dans le dossier d'audit sous-jacent);

iv. les certifications soient délivrées et les audits soient effectués sur la base de normes largement reconnues et qu'ils incluent un test relatif à l'efficacité opérationnelle des contrôles clés en place;

v. l'établissement pratiquant l'externalisation ait le droit contractuel de demander l'extension du périmètre des certifications ou des rapports d'audit à certains systèmes et/ou 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.

9. Compte tenu du niveau élevé de complexité technique des solutions en nuage, l'établissement pratiquant l'externalisation devrait vérifier que le personnel chargé de l'audit – qu'il s'agisse de ses auditeurs internes ou de l'équipe d'auditeurs agissant en son nom, ou des auditeurs désignés par le fournisseur de services en nuage – ou, le cas échéant, le personnel qui examine la certification par un tiers ou les rapports d'audit du fournisseur de services, aient acquis les connaissances et les compétences adéquates pour procéder à une évaluation et/ou à un audit efficaces et pertinents des solutions en nuage.

En ce qui concerne les autorités compétentes

10. Sur la base de l'orientation 8, paragraphe 2, point h), des orientations du CECB et aux fins de l'externalisation en nuage, les établissements pratiquant l'externalisation devraient veiller à disposer d'un accord écrit avec le fournisseur de services en nuage, par lequel ce dernier s'engage à:

    (a) fournir à l'autorité compétente qui supervise l'établissement pratiquant l'externalisation (ou à tout tiers désigné à cet effet par cette autorité) un accès complet aux locaux professionnels du fournisseur de services en nuage (siège social et centres opérationnels), y compris à l'ensemble des dispositifs, systèmes, réseaux et données utilisés pour la fourniture des services à l'établissement pratiquant l'externalisation (droit d'accès);

    (b) conférer à l'autorité compétente qui supervise l'établissement pratiquant l'externalisation (ou à tout tiers désigné à cet effet par cette autorité) des droits illimités en matière d'inspection et d'audit des services externalisés (droit d'audit).

11. L'établissement pratiquant l'externalisation devrait veiller à ce que les arrangements contractuels n'empêchent pas son autorité compétente d'exercer sa fonction de supervision et d'atteindre ses objectifs.

12. Les informations obtenues par les autorités compétentes dans l'exercice de leurs droits d'accès et d'audit devraient être soumises aux exigences en matière de secret professionnel et de confidentialité visées aux articles 53 et suivants de la directive 2013/36/UE (4E directive sur les exigences de fonds propres). Les autorités compétentes devraient s'abstenir de conclure tout type d'accord contractuel ou de déclaration qui les empêcherait de respecter les dispositions du droit de l'Union relatives à la confidentialité, au secret professionnel et à l'échange d'informations.

13. Sur la base des conclusions de son audit, l'autorité compétente devrait traiter toute lacune constatée, le cas échéant, en imposant directement des mesures à l'établissement pratiquant l'externalisation.

4.4 En ce qui concerne le droit d'accès

14. L'accord visé aux points 6 et 10 devrait inclure les dispositions suivantes:

(a) la partie qui entend exercer son droit d'accès (établissement, autorité compétente, auditeur ou tiers agissant pour le compte de l'établissement ou de l'autorité compétente) devrait annoncer, avant toute planification de visite sur place et dans un délai raisonnable, sa visite sur place des locaux professionnels concernés, à moins qu'une notification préalable anticipée n'ait pas été possible en raison d'une situation d'urgence ou de crise;

(b) le fournisseur de services en nuage est tenu de coopérer pleinement avec les autorités compétentes concernées, ainsi qu'avec l'établissement et son auditeur, dans le cadre de la visite sur place.

4.5 Sécurité des données et systèmes

15. Conformément à l'orientation 8, paragraphe 2, point e), des orientations du CECB, le contrat d'externalisation devrait obliger le fournisseur de services externes à protéger la confidentialité des informations transmises par l'établissement financier. En vertu de l'orientation 6, paragraphe 6, point e), des orientations du CECB, les établissements devraient mettre en place des dispositions visant à assurer la continuité des services fournis par les fournisseurs de services externes. Sur la base de l'orientation 8, paragraphe 2, point b), et de l'orientation 9, des orientations du CECB, les besoins respectifs des établissements pratiquant l'externalisation en matière de qualité et de performance devraient être pris en considération dans les contrats d'externalisation écrits et les accords de niveaux de service. Ces questions liées à la sécurité devraient également faire l'objet d'un suivi permanent (orientation 7).

16. Aux fins du point précédent, avant l'externalisation et afin d'éclairer la prise de décision, l'établissement devrait au moins effectuer les opérations suivantes:

(a) recenser et classifier ses activités, ses processus et les données et systèmes connexes en matière de sensibilité et de protection requise;

(b) procéder à une sélection minutieuse, fondée sur les risques, des activités, des processus et des données et systèmes connexes susceptibles d'être externalisés vers une infrastructure informatique en nuage;

(c) définir et décider d'un niveau approprié de protection de la confidentialité des données, de continuité des activités externalisées, ainsi que d'intégrité et de traçabilité des données et des systèmes dans le cadre de l'externalisation en nuage envisagée. Par ailleurs, les établissements devraient examiner des 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.

17. Par la suite, les établissements devraient veiller à disposer d'un accord écrit avec le fournisseur de services en nuage dans lequel figurent notamment les obligations qui incombent à ce dernier en vertu du paragraphe 16 (c).

18. Les établissements devraient assurer le suivi permanent de l'exécution des activités et des mesures de sécurité, conformément à l'orientation 7 des orientations du CECB, y compris les incidents, et, le cas échéant, vérifier si l'externalisation de leurs activités est conforme aux points précédents. En outre, ils devraient prendre sans délai les mesures correctrices requises.

4.6 Localisation des données et traitement des données

19. Comme indiqué dans l'orientation 4, paragraphe 4, des orientations du CECB, les établissements devraient prendre des précautions particulières lorsqu'ils concluent et gèrent des accords d'externalisation convenus en dehors de l'EEE, en raison des risques potentiels pour la protection des données et pour le contrôle effectif par l'autorité de surveillance.

20. L'établissement pratiquant l'externalisation devrait adopter une approche fondée sur le risque concernant la localisation et le traitement des données lorsqu'il recourt à l'externalisation vers un environnement en nuage. L'évaluation devrait porter sur la possible incidence des risques, y compris les risques juridiques et les questions de conformité, ainsi que sur les limites de la surveillance dans les pays où les services externalisés sont fournis ou susceptibles de l'être et les données stockées ou susceptibles de l'être. L'évaluation devrait tenir compte de considérations relatives à la stabilité politique et sécuritaire plus large des juridictions en cause, aux lois en vigueur au sein de ces juridictions (y compris la législation relative à la protection des données), et aux dispositions sur l'application des lois en vigueur dans ces juridictions, y compris les dispositions relatives à l'insolvabilité qui s'appliqueraient en cas d'erreur de la part du fournisseur de services en nuage. L'établissement pratiquant l'externalisation devrait veiller à ce que ces risques soient maintenus dans des limites acceptables et proportionnées au caractère significatif de l'activité externalisée.

4.7 Externalisation en chaîne

21. Conformément à l'orientation 10 des orientations du CECB, les établissements devraient prendre en considération les risques associés à l'externalisation «en chaîne», à savoir lorsque le fournisseur de services externe sous-traite une partie des services à d'autres fournisseurs. L'établissement pratiquant l'externalisation ne devrait accepter l'externalisation en chaîne que si le sous-traitant de second rang se conforme lui aussi pleinement aux obligations en vigueur entre l'établissement pratiquant l'externalisation et le fournisseur de services d'externalisation. En outre, l'établissement pratiquant l'externalisation devrait adopter des mesures appropriées pour limiter le risque qu'une faiblesse ou un échec dans la fourniture des activités sous-traitées en chaîne n'entraînent des répercussions significatives sur la capacité du fournisseur de services d'externalisation à s'acquitter des responsabilités qui lui incombent en vertu de l'accord d'externalisation.

22. L'accord d'externalisation conclu entre l'établissement pratiquant l'externalisation et le fournisseur de services en nuage devrait préciser tous les types d'activités exclues d'une potentielle sous-traitance de nième rang et indiquer que le fournisseur de services en nuage assume la pleine responsabilité et le contrôle des services qu'il a lui-même sous-traités.

23. Par ailleurs, l'accord d'externalisation devrait prévoir l'obligation pour le fournisseur de services en nuage d'informer l'établissement pratiquant l'externalisation de tout changement significatif prévu concernant les sous-traitants de nième rang ou les services sous-traités en chaine mentionnés dans l'accord initial qui pourrait affecter la capacité du fournisseur de services à

s'acquitter des responsabilités qui lui incombent en vertu de l'accord d'externalisation. La période de notification de ces changements devrait être convenue au préalable par voie contractuelle afin de permettre à l'établissement pratiquant l'externalisation de procéder à une évaluation des risques liés aux changements suggérés avant que le changement effectif concernant les sous-traitants de nième rang ou les services sous-traités en chaine ne prenne effet.

24. Si un fournisseur de services en nuage envisage des changements concernant un sous-traitant de second-rang ou des services sous-traités en chaine qui pourraient avoir une incidence négative sur l'évaluation des risques des services convenus, l'établissement pratiquant l'externalisation devrait avoir le droit de résilier le contrat.

25. L'établissement pratiquant l'externalisation devrait examiner et contrôler en permanence l'exécution du service global, qu'il soit assuré par le fournisseur de services en nuage ou par ses sous-traitants de nième rang.

4.8 Plans d'urgence et stratégies de retrait

26. Conformément à l'orientation 6.1, à l'orientation 6, paragraphe 6, point e), et à l'orientation 8, paragraphe 2, point d), des orientations du CECB, l'établissement pratiquant l'externalisation devrait prévoir et mettre en œuvre des dispositions visant à maintenir la continuité de ses activités si la prestation de services par un fournisseur de services externe échoue ou se dégrade de manière inacceptable. Ces dispositions devraient inclure des plans d'urgence et une stratégie de retrait clairement définie. Par ailleurs, le contrat d'externalisation devrait prévoir une clause de résiliation et de gestion du retrait permettant de transférer les activités assurées par le fournisseur de services d'externalisation vers un autre fournisseur de services d'externalisation ou de les réintégrer dans l'établissement pratiquant l'externalisation.

27. Un établissement pratiquant l'externalisation devrait également s'assurer qu'il est en mesure de se retirer des arrangements d'externalisation en nuage, si nécessaire, sans que cela n'entrave indûment sa fourniture de services ni n'entraîne d'effets négatifs sur sa conformité au régime réglementaire et sans préjudice de la continuité et de la qualité des services qu'il fournit aux clients. Pour ce faire, l'établissement pratiquant l'externalisation devrait:

    (a) élaborer et mettre en œuvre des plans de retrait complets, documentés et suffisamment testés, le cas échéant;

    (b) définir des solutions de remplacement et élaborer des plans de transition pour lui permettre d'éliminer et de transférer les activités et les données existantes du fournisseur de services en nuage vers ces solutions, d'une manière contrôlée et suffisamment testée, en tenant compte des questions de localisation des données et du maintien de la continuité des activités pendant la phase de transition;

    (c) veiller à ce que l'accord d'externalisation inclut l'obligation pour le fournisseur de services en nuage d'accompagner de manière suffisante l'établissement pratiquant

l'externalisation dans le transfert méthodique de l'activité vers un autre fournisseur de services ou vers la gestion directe de l'établissement pratiquant l'externalisation en cas de résiliation de l'accord d'externalisation.

28. Lorsqu'il élabore des stratégies de retrait, l'établissement pratiquant l'externalisation devrait tenir compte des éléments suivants:

    (a) élaborer des indicateurs de risque clés pour déterminer à partir de quel niveau un niveau de service devient inacceptable;

    (b) réaliser une analyse d'impact sur l'activité adaptée aux activités externalisées afin de déterminer les ressources humaines et matérielles nécessaires à la mise en œuvre du plan de retrait ainsi que le temps requis à cet effet;

    (c) attribuer des fonctions et des responsabilités pour la gestion des plans de retrait et des activités de transition;

    (d) élaborer des critères de réussite de la transition.

29. L'établissement pratiquant l'externalisation devrait inclure des indicateurs en mesure de déclencher le plan de retrait dans son contrôle permanent du service et dans sa surveillance des services fournis par le fournisseur de services en nuage.