TC.1-2a

boulevard de Berlaimont 14 – BE-1000 Bruxelles
tél. +32 2 221 44 74
numéro d'entreprise : 0203.201.340
RPM Bruxelles
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Bruxelles, le 5 mai 2020

Référence : NBB_2020_018

votre correspondant :
Nicolas Strypstein
tél. +32 2 221 44 74
nicolas.strypstein@nbb.be

Recommandations de la Banque relatives à la sous-traitance à des fournisseurs de services en nuage (*cloud services*)

Champ d'application

La présente circulaire s'applique aux :

- *entreprises d'assurance et de réassurance de droit belge soumises à la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance (à l'exception des entreprises d'assurance visées aux articles 275, 276 ou 294 de la loi du 13 mars 2016 précitée) ;*
- *succursales agréées en Belgique d'entreprises d'assurance ayant leur siège social dans un pays tiers (pays qui n'est pas partie à l'accord sur l'Espace économique européen (EEE)) ; et*
- *entités responsables*[1] *d'un groupe d'assurance ou de réassurance de droit belge au sens des articles 339, 2° et 343 de la loi du 13 mars 2016 ou d'un conglomérat financier de droit belge au sens des articles 340, 1° et 343 de la loi du 13 mars 2016.*

Résumé/Objectif

La présente circulaire précise les recommandations de la Banque nationale de Belgique (la Banque) en matière sous-traitance à des fournisseurs de services en nuage (c*loud*). Elle met en en œuvre les orientations de l'Autorité européenne des assurances et des pensions professionnelles (EIOPA) sur ce sujet et sera d'application à partir du 1er janvier 2021.

La présente circulaire stipule également l'approche suivie par la Banque en matière de reporting. A cet égard, elle doit être lue en liaison avec le chapitre 7 de la circulaire coupole en matière de système de gouvernance 2016-31 qui précise les recommandations générales de la Banque en matière de sous-traitance (recommandations qui viennent d'être revues par le biais de la communication NBB_2020_017).

1 Et plus précisément les entreprises d'assurance ou de réassurance de droit belge qui sont une entreprise participante dans au moins une entreprise d'assurance ou de réassurance de l'Espace Economique Européen ou d'un pays tiers, les entreprises d'assurance ou de réassurance de droit belge dont l'entreprise mère est une société holding mixte d'assurance ou une compagnie financière mixte de l'Espace Economique Européen ou d'un pays tiers et les sociétés holding d'assurance ou compagnies financières mixtes de droit belge qui sont entreprises mères d'une entreprise d'assurance ou de réassurance de droit belge dans la mesure où celles-ci sont soumises aux dispositions de la loi du 13 mars 2016.

Madame,
Monsieur,

Conformément à l'article 92 de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance (ci-après la « Loi de contrôle assurance»), chaque entreprise d'assurance ou de réassurance est tenu de prendre des mesures adéquates pour que le recours à la sous-traitance n'entraîne pas une des conséquences suivantes : (i) compromettre gravement la qualité du système de gouvernance de l'entreprise, (ii) accroître indûment le risque opérationnel, (iii) empêcher la Banque nationale de Belgique (la « Banque ») de vérifier si l'entreprise respecte ses obligations légales et règlementaires et (iv) nuire à la prestation continue d'un niveau de service satisfaisant à l'égard des preneurs d'assurance, des assurés et des bénéficiaires de contrats d'assurance ou des personnes concernés par l'exécution des contrats de réassurance.

Les règles générales en matière de sous-traitance sont explicitées à l'article 274 du Règlement délégué 2015/35 du 10 octobre 2014 complétant la directive Solvabilité II (ci-après, « Règlement délégué 2015/35 ») et dans le chapitre 7 de la circulaire coupole en matière de système de gouvernance 2016/31 (chapitre qui a été récemment mis-à-jour par le biais de la communication NBB_2020_017).

Par la présente circulaire, la Banque entend communiquer des recommandations complémentaires particulières pour le cas spécifique de la sous-traitance à des fournisseurs de services en nuage (*cloud*). Ces recommandations traduisent dans l'environnement réglementaire belge les « *Guidelines on outsourcing to cloud service providers* » publiées par l'EIOPA le 6 février 2020.

1. Recommandations de la Banque

Définitions

Aux fins de la présente circulaire, les définitions suivantes s'appliquent :

- « entreprise » : entreprise d'assurance ou de réassurance visées dans le champ d'application repris ci-dessus ;
- « prestataire de services » : tiers exécutant tout ou partie d'une procédure, d'un service ou d'une activité au titre d'un dispositif de sous-traitance ;
- « prestataire de services en nuage » : prestataire de services, tel que défini ci-dessus, chargé de fournir des services en nuage au titre d'un dispositif de sous-traitance ;
- « 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 une seule entreprise en vue d'une utilisation exclusive ;
- « nuage communautaire » : infrastructure en nuage accessible à une communauté d'entreprises précise, par exemple à plusieurs entreprises d'un même groupe, en vue d'une utilisation exclusive ;
- « nuage hybride » : infrastructure en nuage composée d'au moins deux infrastructures en nuage distinctes.

Recommandation 1 – Services en nuage et sous-traitance

L'entreprise détermine si un dispositif conclu avec un prestataire de services en nuage relève de la définition de la sous-traitance conformément à la Loi de contrôle assurance.

Dans le cadre de cette évaluation, il convient d'examiner :
a. si la fonction ou activité opérationnelle (ou une partie de celle-ci) sous-traitée est exercée de manière récurrente ou continue ; et
b. si cette fonction ou activité opérationnelle (ou une partie de celle-ci) relève normalement de fonctions ou activités opérationnelles qui seraient ou pourraient être exercées par l'entreprise dans le cadre de ses activités d'assurance ou de réassurance régulières, même si l'entreprise n'a pas exercé cette fonction ou activité opérationnelle par le passé.

Lorsqu'un dispositif conclu avec un prestataire de services couvre plusieurs fonctions ou activités opérationnelles, l'entreprise devrait tenir compte de tous les aspects du dispositif dans son évaluation.

Dans les cas où l'entreprise sous-traite des fonctions ou activités opérationnelles à des prestataires de services qui ne sont pas des prestataires de services en nuage mais qui dépendent largement des infrastructures en nuage pour fournir leurs services (par exemple, lorsque le prestataire de services en nuage fait partie d'une chaîne de sous-sous-traitance), le dispositif relatif à ce type de sous-traitance relève des présentes Recommandations.

Recommandation 2 – Principes généraux de gouvernance en matière de sous-traitance en nuage

Sans préjudice de l'article 274, paragraphe 3, du Règlement délégué 2015/35, le conseil d'administration et le comité de direction de l'entreprise veillent à ce que toute décision de sous-traiter des fonctions ou activités opérationnelles critiques ou importantes à des prestataires de services en nuage s'appuie sur une évaluation approfondie des risques, y compris tous les risques pertinents inhérents au dispositif, tels que les risques liés aux technologies de l'information et de la communication (« ICT »), les risques en matière de continuité de l'activité, les risques juridiques et de compliance (y compris la confidentialité), les risques de concentration, d'autres risques opérationnels, et les risques associés à la migration des données et /ou à la phase de mise en œuvre, le cas échéant.

En cas de sous-traitance de fonctions ou activités opérationnelles critiques ou importantes à des prestataires de services en nuage, l'entreprise reflète, lorsque c'est approprié, dans son évaluation interne des risques et de la solvabilité (*Own Risk and Solvency Assessment*, ORSA) les modifications apportées à son profil de risque en raison de ses dispositifs de sous-traitance en nuage.

L'utilisation de services en nuage est cohérente par rapport aux stratégies (par exemple, la stratégie en matière d' « ICT », la stratégie en matière de sécurité de l'information, la stratégie de gestion du risque opérationnel) ainsi qu'aux politiques et processus internes de l'entreprise, qui devraient, si nécessaire, être mis à jour.

Recommandation 3 – Mise à jour de la politique écrite en matière de sous-traitance

En cas de sous-traitance à des prestataires de services en nuage, l'entreprise met à jour la politique **écrite en matière de sous-traitance** (par exemple, en la révisant, en ajoutant une annexe distincte ou en élaborant de nouvelles politiques dédiées) et les autres politiques internes pertinentes (par exemple, en matière de sécurité de l'information), en prenant en compte les spécificités de la sous-traitance en nuage au moins dans les domaines suivants :

a. les missions et responsabilités des fonctions concernées de l'entreprise, en particulier le conseil d'administration et le comité de direction, et les fonctions chargées des « ICT », de la sécurité de l'information, de la compliance, de la gestion des risques et de l'audit interne ;
b. les processus et les procédures de reporting requis pour l'approbation, la mise en œuvre, le contrôle, la gestion et le renouvellement, le cas échéant, des dispositifs de sous-traitance en nuage relatifs à des fonctions ou activités opérationnelles critiques ou importantes ;

c. la supervision des services en nuage proportionnellement à la nature, à l'ampleur et à la complexité des risques inhérents aux services fournis, y compris : i. l'évaluation des risques liés aux dispositifs de sous-traitance en nuage et la diligence appropriée à l'égard des prestataires de services en nuage, y compris la fréquence de l'évaluation des risques, ii. les contrôles de suivi et de gestion (par exemple, la vérification de l'accord de niveau de service), iii. les normes et contrôles de sécurité ;
d. s'agissant de la sous-traitance en nuage de fonctions ou activités opérationnelles critiques ou importantes, il conviendrait de renvoyer aux exigences contractuelles décrites à la Recommandation 8 ;
e. les exigences en matière de documentation et la notification écrite à l'autorité de contrôle en ce qui concerne la sous-traitance en nuage de fonctions ou activités opérationnelles critiques ou importantes ;
f. pour chaque dispositif de sous-traitance en nuage portant sur des fonctions ou activités opérationnelles critiques ou importantes, une exigence de « stratégie de sortie » documentée et, si nécessaire, suffisamment testée qui soit proportionnée à la nature, à l'ampleur et à la complexité des risques inhérents aux services fournis. La stratégie de sortie peut comprendre une série de processus de résiliation incluant, sans nécessairement s'y limiter, l'interruption, la réinternalisation ou le transfert des services contenus dans le dispositif de sous-traitance en nuage.

Recommandation 4 – Analyse préalable à la sous-traitance

Avant de conclure un dispositif avec des prestataires de services en nuage, l'entreprise veille à :

a. évaluer si le dispositif de sous-traitance en nuage concerne une fonction ou activité opérationnelle critique ou importante conformément à la Recommandation 5 ;
b. recenser et évaluer tous les risques pertinents du dispositif de sous-traitance en nuage conformément à la Recommandation 6 ;
c. effectuer les vérifications nécessaires (« due diligence ») à l'égard du prestataire de services en nuage potentiel conformément à la Recommandation 7 ;
d. recenser et évaluer les conflits d'intérêts que la sous-traitance pourrait entraîner conformément aux exigences énoncées à l'article 274, paragraphe 3, point b), du Règlement délégué 2015/35.

Recommandation 5 – Évaluation du caractère critique ou important de la sous-traitance en nuage

Avant de conclure un dispositif de sous-traitance avec des prestataires de services en nuage, l'entreprise évalue si le dispositif de sous-traitance en nuage concerne une fonction ou activité opérationnelle critique ou importante. Lors de la réalisation d'une telle évaluation, l'entreprise examine, lorsque cela est pertinent, si le dispositif a le potentiel de devenir critique ou important à l'avenir. Elle réévalue également le caractère critique ou important de la fonction ou activité opérationnelle précédemment sous-traitée à des prestataires de services en nuage si la nature, l'ampleur et la complexité des risques inhérents à l'accord ont changé de manière significative.

Dans l'évaluation, l'entreprise tient compte, outre des résultats de l'évaluation des risques, au moins des facteurs suivants :

a. l'incidence potentielle de toute perturbation significative de la fonction ou activité opérationnelle sous-traitée ou de l'incapacité du prestataire de services en nuage d'assurer les services aux niveaux convenus en prenant en compte les éléments suivants de l'entreprise : i. le respect constant de ses obligations réglementaires ; ii. sa résilience et sa viabilité financière et en matière de solvabilité à court et à long terme ; iii. la continuité de l'activité et la résilience opérationnelle ; iv. les risques opérationnels, y compris les risques liés à la conduite, les risques liés aux « ICT » et les risques juridiques ; v. les risques de réputation ;

b. l'incidence potentielle du dispositif de sous-traitance en nuage sur la capacité de l'entreprise : i. de recenser, de suivre et de gérer tous les risques pertinents ; ii. de se conformer à toutes les exigences légales et réglementaires ; iii. d'effectuer les audits appropriés concernant la fonction ou activité opérationnelle sous-traitée ;
c. l'exposition globale de l'entreprise (et/ou du groupe, le cas échéant) à un même prestataire de services en nuage et l'incidence cumulative potentielle des dispositifs de sous-traitance dans un même domaine d'activité ;
d. la taille et la complexité de tout domaine d'activité de l'entreprise touché par le dispositif de sous-traitance en nuage ;
e. la capacité, si nécessaire ou souhaitable, de transférer le dispositif de sous-traitance en nuage proposé à un autre prestataire de services en nuage ou de réinternaliser les services (« substituabilité ») ;
f. la protection des données à caractère personnel et non personnel et l'incidence potentielle sur l'entreprise, les preneurs d'assurance ou d'autres sujets pertinents d'une violation de la confidentialité ou d'un manquement à l'obligation de garantir la disponibilité et l'intégrité des données sur la base notamment du règlement (UE) 2016/679. L'entreprise devrait en particulier prendre en compte les données constituant un secret commercial et/ou sensibles (par exemple, les données sur la santé des preneurs d'assurance).

Recommandation 6 – Évaluation des risques liés à la sous-traitance en nuage

De manière générale, l'entreprise adopte une approche proportionnée à la nature, à l'ampleur et à la complexité des risques inhérents aux services sous-traités à des prestataires de services en nuage. Cela inclut l'évaluation de l'incidence potentielle de toute sous-traitance en nuage, en particulier, sur leurs risques opérationnels et de réputation.

En cas de sous-traitance de fonctions ou activités opérationnelles critiques ou importantes à des prestataires de services en nuage, l'entreprise veille à :

a. tenir compte des avantages et des coûts attendus du dispositif de sous-traitance en nuage proposé, notamment en mettant en balance les risques significatifs qui pourraient être réduits ou mieux gérés avec les risques significatifs qui pourraient découler du dispositif de sous-traitance en nuage proposé ;

b. évaluer, dans le cas et dans la mesure où il y a lieu, les risques, y compris les risques juridiques, d'«ICT», de conformité et de réputation, ainsi que les limites en matière de supervision découlant :

   i. du service en nuage sélectionné et des modèles de déploiement proposés (c'est-à-dire en nuage public/privé/hybride/communautaire) ;
   ii. de la migration et/ou de la mise en œuvre ;
   iii. des activités et des données et systèmes connexes dont la sous-traitance est envisagée (ou qui ont été sous-traités) et de leur sensibilité ainsi que des mesures de sécurité requises ;
   iv. de la stabilité politique et de la situation en matière de sécurité des pays (au sein ou en dehors de l'UE) où les services sous-traités sont ou pourraient être fournis et où les données sont stockées ou sont susceptibles de l'être. L'évaluation devrait examiner : 1. les lois en vigueur, notamment les lois sur la protection des données ; 2. les dispositions en vigueur en matière d'application des lois ; 3. les dispositions du droit de 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'entreprise ;
   v. de la sous-sous-traitance, y compris des risques supplémentaires qui peuvent survenir si le sous-sous-traitant est situé dans un pays tiers ou dans un pays autre que celui du prestataire de services en nuage, et du risque que des chaînes longues et complexes de sous-sous-traitance réduisent la capacité de l'entreprise de contrôler ses fonctions ou activités opérationnelles critiques ou importantes et la capacité des autorités de contrôle de les surveiller efficacement ;

vi. du risque de concentration global de l'entreprise envers un même prestataire de services en nuage, y compris la sous-traitance à un prestataire de services en nuage qui n'est pas facilement substituable ou des dispositifs de sous-traitance multiples conclus avec le même prestataire de services en nuage.

Lorsqu'elle évalue le risque de concentration, l'entreprise (et/ou le groupe, le cas échéant) tient compte de tous ses dispositifs de sous-traitance conclus avec ce prestataire de services en nuage.

L'évaluation des risques est effectuée avant de conclure une sous-traitance en nuage. Si l'entreprise vient à avoir connaissance de lacunes importantes et/ou de modifications significatives dans les services fournis ou dans la situation du prestataire de services en nuage, l'évaluation des risques est révisée ou réexécutée rapidement. En cas de renouvellement d'un dispositif de sous-traitance en nuage portant sur son contenu et son champ d'application (par exemple, l'élargissement du champ d'application ou l'inclusion dans le champ d'application de fonctions opérationnelles critiques ou importantes précédemment non incluses), l'évaluation des risques est effectuée à nouveau.

Recommandation 7 – Diligence appropriée à l'égard du prestataire de services en nuage

L'entreprise s'assure, dans son processus de sélection et d'évaluation, que le prestataire de services en nuage est apte à fournir les services en question selon les critères définis par sa politique écrite en matière de sous-traitance (processus de « due diligence »).

La diligence appropriée à l'égard du prestataire de services en nuage est exercée préalablement à la mise en place de la sous-traitance de toute fonction ou activité opérationnelle. Au cas où l'entreprise conclue un deuxième accord avec un prestataire de services en nuage ayant déjà fait l'objet d'une évaluation, l'entreprise détermine, selon une approche fondée sur les risques, si une deuxième diligence appropriée est nécessaire. Si l'entreprise vient à avoir connaissance de lacunes importantes et/ou de modifications significatives dans les services fournis ou dans la situation du prestataire de services en nuage, la diligence appropriée est révisée ou réexécutée rapidement.

En cas de sous-traitance en nuage de fonctions opérationnelles critiques ou importantes, la diligence appropriée inclut une évaluation de l'aptitude du prestataire de services en nuage (par exemple, les compétences, l'infrastructure, la situation économique, le statut de l'entreprise le statut réglementaire). Le cas échéant, l'entreprise peut avoir recours, pour soutenir la diligence appropriée exécutée, à des éléments probants, à des certifications basées sur des normes internationales ou à des rapports d'audit internes ou effectués par des tiers reconnus.

Recommandation 8 - Exigences contractuelles

Les droits et obligations respectifs de l'entreprise et du prestataire de services en nuage devraient être clairement répartis et définis dans un accord écrit.

Sans préjudice des exigences définies à l'article 274 du règlement délégué, en cas de sous-traitance de fonctions ou activités opérationnelles critiques ou importantes à un prestataire de services en nuage, l'accord écrit entre l'entreprise et le prestataire de services en nuage devrait comporter les éléments suivants :

a. une description claire de la fonction sous-traitée à assurer (services en nuage, y compris le type de services de soutien) ;
b. la date de début et de fin de l'accord, le cas échéant, et les délais de préavis pour le prestataire de services en nuage et pour l'entreprise ;
c. la compétence judiciaire et la législation applicable régissant l'accord ;

d. les obligations financières des parties ;
e. la sous-traitance en cascade d'une fonction ou activité opérationnelle critique ou importante (ou de parties significatives de celle-ci), est-elle autorisée ou non et, dans l'affirmative, quelles sont les conditions qui sont applicables à la sous-sous-traitance significative (voir Recommandation 13) ;
f. le(s) lieu(x) (c.-à-d. les régions ou pays) où les données pertinentes seront conservées et traitées, (lieu des centres de données), et les conditions à remplir, y compris l'obligation d'informer l'entreprise si le prestataire de services envisage de modifier le(s) lieu(x) ;
g. les dispositions concernant l'accessibilité, la disponibilité, l'intégrité, la confidentialité, le caractère privé et la sécurité des données pertinentes, compte tenu des spécifications de la Recommandation 10 ;
h. le droit de l'entreprise de contrôler régulièrement les performances du prestataire de services en nuage ;
i. les niveaux de service convenus, qui devraient inclure des objectifs de performance quantitatifs et qualitatifs précis afin de permettre un suivi en temps opportun, de sorte que des mesures correctives appropriées puissent être prises sans délai indu si les niveaux de service convenus ne sont pas respectés ;
j. les obligations de déclaration du prestataire de services en nuage envers l'entreprise, y compris, le cas échéant, l'obligation de présenter des rapports pertinents pour la fonction de sécurité et les fonctions clés de l'entreprise, tels que les rapports de la fonction d'audit interne du prestataire de services en nuage :
k. le prestataire de services en nuage devrait-il souscrire une assurance obligatoire contre certains risques et, le cas échéant, quel est le niveau de couverture d'assurance demandé ;
l. les exigences relatives à la mise en œuvre et à la mise à l'essai des plans d'urgence de l'activité ;
m. l'obligation pour le prestataire de services en nuage d'accorder à l'entreprise, à ses autorités de contrôle et à toute autre personne désignée par l'entreprise ou les autorités de contrôle, les droits suivants : i. un accès total à tous les locaux opérationnels pertinents (sièges sociaux et centres d'exploitation), y compris à l'ensemble des dispositifs, systèmes, réseaux, informations et données utilisés pour assurer la fonction sous-traitée, en ce compris les informations financières, le personnel et les auditeurs externes du prestataire de services en nuage (« droits d'accès ») ; ii. les droits illimités d'inspection et d'audit liés à l'accord de sous-traitance en nuage (« droits d'audit »), afin de leur permettre de veiller aux modalités de la sous-traitance et de garantir le respect de l'ensemble des exigences réglementaires et contractuelles applicables ;
n. des dispositions garantissant la récupération rapide des données détenues par l'entreprise en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du prestataire de services en nuage.

Recommandation 9 - Droits d'accès et d'audit

L'accord de sous-traitance en nuage ne devrait pas limiter l'exercice effectif par l'entreprise de ses droits d'accès et d'audit, ni ses possibilités de contrôle des services en nuage aux fins du respect de ses obligations réglementaires.

L'entreprise devrait exercer ses droits d'accès et d'audit et déterminer la fréquence des audits et les domaines et services à auditer selon une approche fondée sur les risques.

Pour déterminer la fréquence et l'étendue de l'exercice de ses droits d'accès ou d'audit, l'entreprise devrait examiner si la sous-traitance en nuage est liée à une fonction ou activité opérationnelle critique ou importante, et quelles sont la nature et l'étendue du risque ainsi que l'incidence sur l'entreprise des accords de sous-traitance en nuage.

Si l'exercice de ses droits d'accès ou d'audit, ou l'utilisation de certaines techniques d'audit, crée un risque pour l'environnement du prestataire de services en nuage et/ou d'un autre client du même prestataire de services en nuage (par exemple, une incidence sur les niveaux de service, sur la disponibilité des données, sur les aspects de confidentialité), l'entreprise et le prestataire de services en nuage devraient convenir d'autres moyens de fournir à l'entreprise un niveau d'assurance et de service similaire (par exemple, l'inclusion de contrôles spécifiques à tester dans un rapport ou une certification spécifique produit(e) par le prestataire de services en nuage).

Sans préjudice de leur responsabilité finale concernant les activités exercées par leurs prestataires de services en nuage, les entreprises peuvent, afin d'utiliser les ressources d'audit de manière plus efficace et de réduire la charge organisationnelle pesant sur le prestataire de services en nuage et ses clients, recourir aux éléments suivants :

a. des certifications de tiers, et des rapports d'audit interne ou d'audits effectués par des tiers, mis à disposition par le prestataire de services en nuage ;
b. des audits groupés (c'est-à-dire réalisés conjointement avec d'autres clients du même prestataire de services en nuage), ou des audits groupés réalisés par un tiers désigné par eux.

En cas de sous-traitance dans le nuage de fonctions ou activités opérationnelles critiques ou importantes, les entreprises ne devraient recourir à la méthode consistant à recourir à des certifications de tiers et des rapports d'audit interne ou d'audits effectués par des tiers que si elles :

a. s'assurent que la portée de la certification ou du rapport d'audit couvre les systèmes (par exemple, les processus, les applications, l'infrastructure, les centres de données, etc.) et les contrôles recensés par l'entreprise et évaluent la conformité par rapport aux exigences réglementaires pertinentes ;
b. évaluent régulièrement et de manière approfondie le contenu des nouvelles certifications ou des nouveaux rapports d'audit et vérifient que les certifications ou rapports ne sont pas obsolètes ;
c. veillent à ce que les systèmes et contrôles clés soient couverts dans les futures versions de la certification ou du rapport d'audit ;
d. ont acquis une certitude raisonnable quant à la compétence de la partie qui procède à la certification ou à l'audit (par exemple en ce qui concerne la rotation de la société de certification ou d'audit, les qualifications, l'expertise, la réexécution/vérification des éléments probanats dans le dossier d'audit sous-jacent) ;
e. ont acquis une certitude raisonnable que les certifications sont délivrées et les audits effectués conformément aux normes appropriées et comprennent un test de l'efficacité opérationnelle des contrôles clés mis en place ;
f. ont le droit contractuel de demander l'extension de la portée des certifications ou rapports d'audit à d'autres systèmes et contrôles pertinents ; le nombre et la fréquence de ces demandes de modification de la portée devraient être raisonnables et légitimes sous l'angle de la gestion des risques ;
g. conservent le droit contractuel d'effectuer des audits individuels sur place à leur discrétion en ce qui concerne la sous-traitance dans le nuage de fonctions ou activités opérationnelles critiques ou importantes ; ce droit devrait être exercé en cas de besoins spécifiques qui ne peuvent être satisfaits par d'autres types d'interactions avec le prestataire de services dans le nuage.

Pour la sous-traitance de fonctions opérationnelles critiques ou importantes à des prestataires de services dans le nuage, l'entreprise devrait évaluer si les certifications et rapports de tiers visés au paragraphe 5 a) de la présente recommandation sont adéquats et suffisants pour respecter ses obligations réglementaires et, selon une approche fondée sur les risques, ne devrait pas se fonder uniquement sur ces rapports et certificats au fil du temps.

Avant une visite sur place planifiée, la partie exerçant son droit d'accès (l'entreprise, l'auditeur ou le tiers agissant au nom de l'entreprise ou des entreprises) devrait prévoir un délai raisonnable entre l'annonce de sa venue et la visite effective, à moins qu'une notification préalable n'ait pas été possible en raison d'une situation d'urgence ou de crise. L'annonce devrait indiquer le lieu et la finalité de la visite ainsi que le personnel qui y participera.

Étant donné que les solutions en nuage présentent un niveau élevé de complexité technique, l'entreprise devrait vérifier que le personnel procédant à l'audit - c'est-à-dire son personnel interne ou le groupe d'auditeurs agissant en son nom, ou les auditeurs désignés par le prestataire de services en nuage - ou, le cas échéant, le personnel chargé d'examiner la certification fournie par la tierce partie ou les rapports d'audit du prestataire de services, ont acquis les compétences et connaissances appropriées pour réaliser les audits et/ou évaluations pertinents.

Recommandation 10 - Sécurité des données et des systèmes

L'entreprise devrait veiller à ce que les fournisseurs de services en nuage respectent les réglementations européennes et nationales ainsi que les normes de sécurité appropriées en matière d'«ICT».

En cas de sous-traitance de fonctions ou activités opérationnelles critiques ou importantes à des fournisseurs de services en nuage, l'entreprise devrait en outre définir des exigences spécifiques en matière de sécurité des informations dans le contrat de sous-traitance, et contrôler régulièrement le respect de ces exigences.

Aux fins du paragraphe précédent, en cas de sous-traitance de fonctions ou activités opérationnelles critiques ou importantes à des prestataires de services en nuage, l'entreprise, appliquant une approche fondée sur les risques et tenant compte de ses responsabilités et de celles du prestataire de services en nuage, devrait :

a. convenir d'une répartition claire des rôles et responsabilités entre le prestataire de services en nuage et l'entreprise en ce qui concerne les fonctions ou activités opérationnelles concernées par la sous-traitance en nuage, et prévoir des délimitations claires entre ces différentes fonctions et activités ;
b. définir et décider d'un niveau approprié de protection des données confidentielles, de la continuité des activités sous-traitées, ainsi que de l'intégrité et de la traçabilité des données et des systèmes dans le contexte de la sous-traitance en nuage envisagée ;
c. envisager des mesures spécifiques, selon les nécessités, pour les données en transit, les données en mémoire et les données au repos, par exemple l'utilisation de technologies de cryptage en combinaison avec une gestion appropriée des clés ;
d. envisager les mécanismes d'intégration des services en nuage avec les systèmes des entreprises, par exemple les interfaces de programmation d'applications et un processus sain de gestion des utilisateurs et des accès ;
e. veiller contractuellement à ce que la disponibilité du trafic du réseau et la capacité prévue répondent à de fortes exigences de continuité, dans les domaines applicables et en fonction de la faisabilité ;
f. définir et décider des exigences de continuité appropriées garantissant des niveaux adéquats à chaque niveau de la chaîne technologique, là où cela est applicable ;
g. disposer d'un processus de gestion des incidents solide et bien documenté, qui couvre les responsabilités respectives, par exemple par la définition d'un modèle de coopération en cas d'incidents effectifs ou soupçonnés ;
h. adopter une approche fondée sur les risques en ce qui concerne le stockage des données et le(s) lieu(x) de traitement des données (c'est-à-dire le pays ou la région) et les considérations de sécurité de l'information ;
i. contrôler le respect des exigences relatives à l'efficacité et à l'efficience des mécanismes de contrôle mis en œuvre par le prestataire de services en nuage qui permettraient d'atténuer les risques liés aux services fournis ;

j. veiller à ce qu'une copie des données soit stockée dans un ou plusieurs emplacements hors du site principal du fournisseur de services en nuage, qui sont sécurisés et suffisamment éloignés du site principal pour ne pas être exposé aux mêmes risques, et envisager -pour des données critiques- la faisabilité de disposer d'une copie indépendamment du fournisseur de services en nuage afin de pouvoir reprendre les activités en cas de défaillance permanente du fournisseur ;
k. veiller à ce que les accès des administrateurs des services dans le nuage soient protégés par des solutions d'authentification forte ;
l. veiller contractuellement à ce que les administrateurs du fournisseur des services dans le nuage ne disposent pas d'accès permanents à ses systèmes et données, conformément au principe de « *least privilege* » ;
m. envisager la mise en place de solutions adéquates afin d'empêcher toute exposition non souhaitée du trafic des données entre l'entreprise et le service dans le nuage.

Recommandation 11 – Sous-traitance en cascade

Si la sous-sous-traitance de fonctions opérationnelles critiques ou importantes (ou d'une partie de celles-ci) est autorisée, l'accord de sous-traitance en nuage entre l'entreprise et le prestataire de services en nuage devrait :

a. spécifier tous les types d'activités qui sont exclus d'une éventuelle sous-sous-traitance ;
b. indiquer les conditions à respecter en cas de sous-sous-traitance (par exemple, que le sous-sous-traitant respectera aussi pleinement les obligations pertinentes du prestataire de services en nuage). Ces obligations comprennent les droits d'audit et d'accès et la sécurité des données et des systèmes ;
c. indiquer que le prestataire de services en nuage conserve l'entière responsabilité et la supervision des services sous-sous-traités ;
d. inclure une obligation pour le prestataire de services en nuage d'informer l'entreprise de toute modification importante apportée aux sous-sous-traitants ou aux services sous-sous-traités qui pourrait entamer la capacité du prestataire de services à remplir ses obligations dans le cadre de l'accord de sous-traitance en nuage. Le délai de notification de ces modifications devrait permettre à l'entreprise, à tout le moins, de procéder à une évaluation des risques des effets des modifications envisagées avant que les modifications effectives apportées aux sous-sous-traitants ou aux services sous-sous-traités n'entrent en vigueur ;
e. garantir, dans les cas où un prestataire de services en nuage prévoit des modifications à un sous-sous-traitant ou à des services sous-sous-traités qui auraient un effet négatif sur l'évaluation des risques des services convenus, que l'entreprise a le droit de s'opposer à ces modifications et/ou le droit de résilier le contrat et de s'en retirer.

Recommandation 12 - Suivi et supervision des accords de sous-traitance en nuage

L'entreprise devrait assurer un suivi régulier de la réalisation, par ses fournisseurs de services en nuage, des activités, des mesures de sécurité et du respect du niveau de service convenu, selon une approche fondée sur les risques. L'accent devrait être mis sur la sous-traitance des fonctions opérationnelles critiques et importantes.

Pour ce faire, l'entreprise devrait mettre en place des mécanismes de suivi et de supervision qui devraient tenir compte, lorsque cela est possible et approprié, de la présence d'une sous-sous-traitance de fonctions opérationnelles critiques ou importantes ou d'une partie de celles-ci.

Le comité de direction devrait périodiquement recevoir des informations à jour sur les risques recensés dans le cadre de la sous-traitance en nuage de fonctions ou activités opérationnelles critiques ou importantes.

Afin d'assurer un suivi et une supervision adéquats de leurs accords de sous-traitance en nuage, les entreprises devraient employer suffisamment de ressources ayant les compétences et les connaissances adéquates pour assurer le suivi des services sous-traités en nuage. Le personnel de l'entreprise chargé de ces activités devrait posséder les connaissances en matière d'«ICT» et de gestion d'entreprise jugées nécessaires.

Recommandation 13 - Droits de résiliation et stratégies de sortie

En cas de sous-traitance en nuage de fonctions ou activités opérationnelles critiques ou importantes, l'entreprise devrait prévoir, dans le cadre de l'accord de sous-traitance en nuage, une clause de stratégie de sortie clairement définie qui lui permette de mettre fin à l'accord si cela s'avère nécessaire. Il faudrait prévoir une possibilité de résiliation sans nuire à la continuité et à la qualité des services fournis aux assurés. Pour ce faire, l'entreprise devrait :

a. élaborer des plans de sortie qui soient bien complets, basés sur les services, documentés et suffisamment testés (par exemple par une analyse, en matière de coûts potentiels, d'incidences, de ressources et des implications sur le plan du calendrier, des différentes options de sortie possibles) ;
b. recenser les solutions alternatives et élaborer des plans de transition appropriés et réalisables pour permettre à l'entreprise d'extraire des activités et données existantes du prestataire de services en nuage pour les transférer à d'autres fournisseurs de services ou les relocaliser au sein de l'entreprise. Ces solutions devraient être définies en tenant compte des difficultés qui peuvent survenir en raison de la localisation des données, en prenant les mesures nécessaires pour assurer la continuité des activités pendant la phase transitoire ;
c. s'assurer que le prestataire de services en nuage apporte un soutien adéquat à l'entreprise lors du transfert, à un autre prestataire de services ou directement à l'entreprise, des données, systèmes ou applications précédemment sous-traités ;
d. convenir avec le prestataire de services en nuage qu'une fois retransférées à l'entreprise, ses données seront supprimées de manière complète et sûre par le prestataire de services en nuage dans toutes les régions.

Dans l'élaboration des stratégies de sortie, l'entreprise devrait envisager :

a. de définir les objectifs de la stratégie de sortie ;
b. de définir les événements déclencheurs (par exemple, des indicateurs de risque clés signalant un niveau de service inacceptable) qui pourraient activer la stratégie de sortie ;
c. d'effectuer une analyse d'incidence sur l'activité qui soit proportionnelle aux activités sous-traitées afin de déterminer quelles ressources humaines et autres, et combien de temps, seraient nécessaires à la mise en œuvre du plan de sortie ;
d. d'attribuer les rôles et les responsabilités pour la gestion des plans de sortie et des activités transitoires ;
e. de définir les critères de réussite de la transition.

Recommandation 14 - Sous-traitance en nuage vers un pays tiers

Sans préjudice de ce qui est prévu à la section 7.4.3. de la circulaire coupole gouvernance, une sous-traitance à un fournisseur de services en nuage dont les données sont localisées hors de l'Espace Economique Européen (hors EEE ou pays tiers) est autorisée à condition que l'entreprise puisse expressément garantir qu'elle-même, son commissaire réviseur agréé et la Banque peuvent exercer et faire appliquer leurs droits de regard et d'examen (audit), et ce conformément à l'article 307 de la Loi de contrôle assurance. Ceci suppose que l'entreprise, son commissaire réviseur agréé et la Banque puissent avoir accès à tout moment en Belgique aux données qui sont localisées hors de l'EEE.

Outre cette règle générale, si la sous-traitance en nuage vers un fournisseur de services dont les données sont localisées dans un pays tiers est considérée comme critique ou importante, elle ne peut être effectuée que si les conditions suivantes sont remplies :

a. il existe un accord de coopération entre la Banque et l'autorité de contrôle prudentielle du pays tiers où les données sont localisées ou, si le fournisseur de services en nuage fait partie d'un groupe soumis à un contrôle au niveau du groupe conformément à la directive 2009/138/CE (article 343 de la Loi de contrôle assurance), il existe un accord de coordination relatif à un collège de supervision auquel la Banque et l'autorité de contrôle prudentielle de ce pays tiers sont parties ; et

b. l'accord de coopération ou de coordination visé au point a. garantit que la Banque est au moins en mesure, d'une part, d'obtenir, sur demande, les informations nécessaires à l'accomplissement de ses missions et, d'autre part, d'obtenir un accès approprié aux données, documents, locaux ou personnel du pays tiers qui sont pertinents pour l'exercice de ses pouvoirs de contrôle (article 307 de la Loi de contrôle assurance).

Ces 2 conditions ne doivent néanmoins pas être remplies si le fournisseur de services en nuage dont les données sont localisées dans un pays tiers rend ces données accessibles et auditables depuis une filiale ou une succursale située dans l'EEE.

Recommandation 15 - Conservation de documents d'assurance

Des règles particulières s'appliquent si la sous-traitance en nuage porte sur la conservation des originaux (i) des contrats d'assurance ou de réassurance (polices et avenants), (ii) des courriers envoyés aux preneurs d'assurance et (iii) des reportings prudentiels requis en vertu de la Loi de contrôle assurance et de ceux requis en vertu de la loi du 4 avril 2014 relative aux assurances.

En effet, l'article 76 de la Loi de contrôle assurance prévoit que cette conservation doit se faire au siège de l'entreprise ou à un autre lieu préalablement autorisé par la Banque en concertation avec la FSMA.

Ainsi, les entreprises qui ont l'intention de recourir à des fournisseurs de services en nuage pour conserver les documents précités sont tenues de respecter non seulement les règles de la présente circulaire mais également celles additionnelles élaborées par la Banque en matière de conservation des documents d'assurance.

2. Documentation et reporting à la Banque

2.1. Documentation interne

Comme indiqué au point 7.6. de la circulaire coupole gouvernance, il est conseillé aux entreprises qui recourent à la sous-traitance de tenir un registre comprenant des informations sur tous leurs dispositifs de sous-traitance (critiques/importants ou non). S'agissant plus particulièrement de la sous-traitance en nuage, il est conseillé à l'entreprise de garder une trace de ces dispositifs dans ce registre (tenu à jour au fil du temps). Il est également conseillé à l'entreprise de garder une trace des dispositifs de sous-traitance en nuage résiliés et de la conserver pendant une période de rétention appropriée. L'entreprise met à la disposition de la Banque, à sa demande, toutes les informations nécessaires à cette dernière pour lui permettre d'assurer la surveillance de l'entreprise, y compris une copie de l'accord de sous-traitance.

2.2. Reporting à la Banque

Les obligations générales en matière de reporting en matière de sous-traitance sont reprises à la section 7.6. de la circulaire coupole gouvernance.

2.2.1. Liste des sous-traitances critiques ou importantes

Les sous-traitances en nuage considérés comme critiques ou importants doivent faire partie de la liste des sous-traitances critiques ou importantes à transmettre à la Banque de manière continue via la plate-forme eCorporate (reporting B.9 repris dans la communication eCorporate).

Les informations à reprendre dans cette liste pour tous les autres cas de sous-traitance critique ou importante (cf. section 7.6. de la circulaire coupole gouvernance) sont également applicables pour les sous-traitances en nuage considérées comme critiques ou importantes. Néanmoins, les informations additionnelles doivent être reprises :

(i) le fait qu'il s'agit d'une sous-traitance en nuage ;
(ii) la date de l'évaluation des risques la plus récente et un bref résumé de ses principaux résultats ;
(iii) les dates des derniers audits et des prochains audits prévus, le cas échéant ;
(iv) un résultat de l'évaluation de la substituabilité du prestataire de services en nuage (par exemple, facile, difficile ou impossible); et
(v) si l'entreprise dispose ou non d'une stratégie de sortie en cas de résiliation par l'une ou l'autre partie ou d'interruption des services par le prestataire de services en nuage.

2.2.2. Notification à la Banque

En ce qui concerne la notification préalable à la Banque pour une nouvelle sous-traitance en nuage critique ou importante, le formulaire standard repris en annexe 4 de la circulaire coupole gouvernance s'applique[2]. Pour la sous-traitance en nuage, certaines annexes complémentaires détaillées au point « Annexes - C. » de ce formulaire sont à communiquer à la Banque.

En cas de changements significatifs et/ou d'incidents critiques concernant la sous-traitance en nuage, la Banque demande aussi aux entreprises de l'en informer immédiatement . Cette communication peut se faire via une mise à jour du formualire intitial.

Par ailleurs, conformément aux règles générales en matière de sous-traitance prévues au chapitre 7 de la circulaire coupole gouvernance, il est précisé que le dossier de notification à transmettre à la Banque pour une sous-traitance en nuage importante ou critique devra toujours être accompagné d'un avis du responsable de la fonction Compliance confirmant le respect des normes en matière de gouvernance entourant la sous-traitance et le caractère complet de la notification transmise (cf. annexe 5 de la circulaire coupole gouvernance).

3. Entrée en application

La présente circulaire est d'application à partir du 1er janvier 2021. Cela implique que l'ensemble des sous-traitances conclues, renouvelées ou adaptées par les entreprises d'assurance ou de réassurance à partir de cette date doivent se conformer à la présente circulaire.

S'agissant des sous-traitances en nuage portant sur des fonctions ou activités opérationnelles critiques ou importantes déjà existantes et en cours, les entreprises ont jusqu'au 31 décembre 2022 pour se conformer à la circulaire[3]. Jusqu'à cette date, ces sous-traitances demeurent soumises à la communication 2012_11 relative aux attentes prudentielles en matière de *Cloud computing*. La présente circulaire abrogera donc défiitivement la communication 2012_11 relative aux attentes prudentielles en matière de *Cloud computing* à partir du 1er janvier 2023.

2 Si une sous-traitance en nuage qui, initialement, n'était pas considérée comme critique ou importante le devient après un certain temps, l'entreprise d'assurance est également tenue d'en avertir immédiatement la Banque en lui transmettant le formulaire standard repris en annexe 1.

3 Lorsque l'examen des accords de sous-traitance en nuage portant sur des fonctions ou activités opérationnelles critiques ou importantes n'est pas finalisé au 31 décembre 2022, l'entreprise en informe immédiatemment la Banque en expliquant les mesures prévues pour achever l'examen ou l'éventuelle stratégie de sortie. La Banque peut, le cas échéant, convenir avec l'entreprise d'un délai prolongé pour mener à bien cet examen. S'agissant de l'examen des sous-traitances en nuage ne portant pas sur des fonctions ou activités critiques ou importantes déjà existantes et en cours, l'entreprise doit informer la Banque pour le 31 décembre 2022 de ses intentions en termes de mise conformité avec les *guidelines* EIOPA.

Une copie de la présente est adressée au(x) commissaire(s), réviseur(s) agréé(s) de votre entreprise.

Je vous prie d'agréer, Madame, Monsieur, l'expression de notre considération très distinguée.

Pierre WUNSCH
Gouverneur