boulevard de Berlaimont 14 – BE-1000 Bruxelles
tél. +32 2 221 37 40 – fax + 32 2 221 31 04
numéro d'entreprise : 0203.201.340
RPM Bruxelles
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Bruxelles, le 19 juin 2018

Référence : NBB_2018_20

votre correspondant :

Thomas Bodequin
tél. +32 2 221 53 65 – fax +32 2 221 31 04
thomas.bodequin@nbb.be

Recommandations de l'ABE sur l'externalisation vers des fournisseurs de services en nuage (cloud services)

Champ d'application

La présente circulaire s'applique aux établissements de crédit et aux sociétés de bourse de droit belge, ainsi qu'aux succursales établies en Belgique d'établissements de crédit et de sociétés de bourse qui relèvent du droit d'un État non membre de l'EEE.

Résumé/Objectif

La présente circulaire met en œuvre les recommandations de l'Autorité bancaire européenne (ci-après l'« ABE ») sur l'externalisation vers des fournisseurs de services en nuage et doit être lue conjointement avec la circulaire PPB_2004/5 sur les saines pratiques de gestion en matière de sous-traitance par des établissements de crédit et des entreprises d'investissement[1] et la communication NBB_2012_11 relative aux attentes prudentielles en matière de *Cloud computing*.

Madame,
Monsieur,

Conformément à l'article 66 de la loi du 25 avril 2014 (ci-après la « loi bancaire »), chaque établissement est tenu de prendre des mesures adéquates pour, d'une part, limiter le risque opérationnel afférent à l'externalisation et, d'autre part, ne pas nuire au caractère adéquat des procédures de contrôle interne de l'établissement, ni empêcher l'autorité de contrôle de vérifier si l'établissement respecte ses obligations légales et réglementaires.

Par la présente circulaire, la BNB entend communiquer que les recommandations de l'ABE sur l'externalisation vers des fournisseurs de services en nuage sont intégrées dans son activité de contrôle.

La circulaire comporte un bref résumé des recommandations de l'ABE sur l'externalisation vers des fournisseurs de services en nuage. Les établissements doivent mettre tout en œuvre pour respecter intégralement ces recommandations. Celles-ci sont disponibles dans les deux langues nationales sur le site internet de l'ABE via le lien suivant :
https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

1 L'ABE a l'intention de réviser les lignes directrices du CECB relatives à l'externalisation et d'y intégrer les recommandations sur l'externalisation vers des fournisseurs de services en nuage. Ces nouvelles lignes directrices sont attendues dans le courant de 2019.

Tout comme ces recommandations de l'ABE sur l'externalisation vers des fournisseurs de services en nuage constituent un complément aux orientations du CECB relatives à l'externalisation, la présente circulaire complète le contenu de la circulaire PPB-2004/5 et de la communication NBB_2012_11 de la BNB. Cela implique que la circulaire PPB-2004/5 et la communication 2012_11 continuent toutefois de s'appliquer dans leur intégralité.

La présente circulaire entre en vigueur le 1er juillet 2018.

Bref résumé :

Avant d'externaliser une activité ou une partie de celle-ci, les établissements doivent évaluer le caractère significatif de cette activité. À cet égard, il convient de prêter une attention particulière à l'incidence potentielle qu'aurait une interruption de service, mais également à l'incidence d'une mauvaise prestation de service et d'une violation de la confidentialité ou de la perte de données.

Les établissements souhaitant externaliser une activité qu'ils considèrent comme significative doivent en informer l'autorité de contrôle au préalable. Les recommandations contiennent une liste minimale d'informations à communiquer à l'autorité de contrôle. Cette dernière peut ensuite demander des informations complémentaires[2] si elle l'estime nécessaire.

En outre, les établissements doivent tenir un registre, y compris à l'échelon du groupe le cas échéant, qui contient l'ensemble des externalisations, qu'elles soient considérées ou non comme significatives. Les recommandations comportent une liste minimale des informations qui doivent être contenues dans ce registre. À la demande de l'autorité de contrôle, l'établissement met à disposition ce registre ainsi qu'une copie des accords d'externalisation que l'autorité de contrôle entend examiner.

Par ailleurs, les établissements doivent présenter de solides garanties en matière de droits d'accès et d'audit. À cette fin, ils doivent prévoir des dispositions spécifiques dans les contrats d'externalisation et veiller à ce qu'il n'y ait aucune entrave ou limite aux droits d'accès et d'audit, qu'ils soient exercés par l'établissement lui-même, par l'autorité de contrôle ou par un tiers designé, comme l'auditeur interne ou l'auditeur externe.

Ces droits d'accès et d'audit sont exercés de manière proportionnelle au risque. Compte tenu des particularités des fournisseurs de services en nuage, les recommandations proposent une série d'outils d'audit alternatifs qui peuvent être utilisés pour ces services externalisés : les audits regroupés (*pooled audits*), la certification de tiers et les rapports d'audit interne ou externe (du fournisseur de services en nuage). Les droits d'accès et d'audit tels que décrits ci-dessus continuent toutefois de s'appliquer dans leur intégralité, et ces outils alternatifs ne peuvent être utilisés que s'ils peuvent être considérés comme adéquats. Le lecteur se référera également aux recommandations dans lesquelles il trouvera les exigences minimales.

Les établissements doivent veiller à la continuité et à la qualité des services fournis. À cette fin, ils prennent différentes mesures, dont : (a) une étude préalable à l'externalisation qui vérifie si une activité est apte à être externalisée, et qui analyse la sensibilité des données et des systèmes concernés et leur protection requise, (b) la fixation des besoins en matière de qualité, de continuité et de protection des données, et (c) la supervision des prestations, dont également le suivi des incidents et la prise éventuelle de mesures correctrices.

Les établissements doivent être particulièrement prudents en cas d'externalisation vers des pays hors de l'EEE et veiller à ne pas prendre de risques excessifs en matière de protection des données, et à ce que l'autorité de contrôle puisse effectuer un suivi efficace des activités externalisées. L'établissement doit examiner les éventuels risques juridiques et de conformité liés à l'externalisation vers des pays tiers, y compris en cas de défaillance du fournisseur de services, et doit tenir compte à cet égard de tous les pays

2 Il s'agit en premier lieu des activités pour lesquelles la BNB attend une documentation solide conformément à la circulaire PPB_2004/5, comme notamment l'évaluation approfondie des risques préalable à l'externalisation.

où des services peuvent être fournis et de tous les endroits où les données peuvent être stockées ou traitées.

Lors de la conclusion des contrats d'externalisation, il est précisé quelles activités sont exclues d'une potentielle externalisation en chaîne. En cas d'externalisation en chaîne, le sous-traitant du fournisseur de services est tenu de se conformer aux obligations en vigueur entre l'établissement pratiquant l'externalisation et le fournisseur de services, et l'établissement devrait contrôler de la même manière les services fournis par externalisation en chaîne. L'établissement pratiquant l'externalisation est informé préalablement des changements intervenant dans l'externalisation en chaîne et se voit offrir la possibilité d'évaluer ces changements. Si ces changements augmentent excessivement le risque pour l'établissement, celui-ci peut résilier prématurément le contrat.

Enfin, les établissements doivent disposer de plans d'urgence et de stratégies de retrait, afin qu'ils puissent garantir la continuité et la qualité de la fourniture de services envers leurs clients. Ces plans peuvent par exemple consister en une reprise en gestion propre des activités externalisées ou en un transfert de ces activités vers un autre fournisseur de services. Les établissements doivent accorder l'attention nécessaire, non seulement à la rapidité avec laquelle ces plans peuvent être exécutés, mais aussi aux éventuels obstacles que l'établissement peut rencontrer le cas échéant, notamment en matière de récupération de données auprès des fournisseurs de services.

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

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

Jan Smets
Gouverneur