Le *Cloud computing* ou l'informatique « en nuage » : Approches en matière de réglementation et de surveillance

Rapport de consultation téléphonique
A2ii – AICA

NOV
2019

Les Consultations téléphoniques sont organisées dans le cadre du partenariat entre l'Initiative Accès à l'assurance (A2ii) et l'Association internationale des contrôleurs d'assurance (AICA). Ces consultations constituent une plateforme d'échanges utile pour que les contrôleurs puissent partager leurs expériences et les enseignements relatifs au développement de l'accès à l'assurance.

Introduction

L'utilisation du *cloud computing* est de plus en plus courante dans le secteur financier, y compris dans le secteur des assurances. Parallèlement à l'utilisation croissante des nouvelles technologies numériques, les assureurs sont désormais en mesure d'utiliser les services en nuage pour stimuler l'innovation et soutenir des fonctions essentielles telles que la souscription et le développement de produits. Le *cloud computing* présente des avantages, mais aussi des risques potentiels non négligeables, tels que ceux liés à la sécurité et à la confidentialité des données, ainsi qu'à la vulnérabilité des systèmes informatiques aux cyberattaques.[1] Il est donc important que les autorités de surveillance des assurances prennent en considération les exigences réglementaires et les pratiques de surveillance qui peuvent se révéler nécessaires pour le *cloud computing*.

La contribution des experts sur cet appel à consultation a été préparée par Denise Garcia Ocampo de l'Institut de stabilité financière[2], laquelle a également fait une présentation sur les appels en anglais et en espagnol. Andrea Camargo, de l'A2ii, a présenté l'avis des experts sur l'appel français. Lázaro Cuesta Barberá (Autorité européenne des pensions professionnelles [AEAPP]), Paulo Miller et Gustavo Adolfo Araujo Caldas *(Superintendência de Seguros Privados* (SUSEP), Brésil) ainsi que Sanjeev Chandran (Autorité de régulation prudentielle [PRA] de la Banque d'Angleterre [BOE], Royaume-Uni [RU]) se sont joints à eux pour partager les enseignements tirés de leurs juridictions respectives.

Les paragraphes suivants, jusqu'aux études de cas, sont un résumé du document de FSI Insights intitulé « Approches en matière de réglementation et de surveillance de l'informatique « en nuage » : approches prudentielles émergentes ».[3]

1 Le Conseil de stabilité financière (CSF) a publié un rapport sur « Les dépendances de tiers dans les services de cloud : Considérations sur les implications en matière de stabilité financière » disponible ici : https://www.fsb.org/wp-content/uploads/P091219-2.pdf

2 Financial Stability Institute (FSI)

3 Le document complet peut être consulté ici : https://www.bis.org/fsi/publ/insights13.pdf

Numérisation du secteur de l'assurance

Les technologies numériques transforment différents secteurs de la chaîne de valeur de l'assurance. Les technologies émergentes telles que l'Internet des objets (IoT – *Internet of Things)* et l'analyse avancée (AA – *Advanced Analytics)* fournissent des informations en temps réel et un aperçu détaillé des besoins, des préférences et des comportements à risque des clients. Ces ressources aident les assureurs à adapter leurs produits et leurs tarifs à des profils de clients spécifiques. D'autres applications des technologies telles que l'apprentissage machine (ML – *Machine Learning)* et l'intelligence artificielle (AI – -*Artifical Intelligence)* comme les chatbots (« dialogueurs » ou « agents conversationnels » en français), les conseillers virtuels ou les experts en sinistres virtuels permettent aux assureurs d'automatiser les processus de distribution, de commercialisation, de souscription et de gestion des sinistres. La technologie des grands livres distribués (DLT – *Distributed Ledger Technology)* est utilisée pour accroître l'efficacité, réduire les coûts et diminuer les besoins d'intermédiation.

Le c*loud computing* est un modèle capable de donner un nouvel élan à l'application des technologies numériques grâce à un dispositif efficace, évolutif et souple. Les assureurs sont en mesure de proposer des produits et des services basés sur les données collectées par l'Internet des objets, traitées par l'AA, le ML, l'AI ou structurées par le DLT, en utilisant des réseaux, des serveurs, des stockages, des applications et des services partagés disponibles à la demande, qui peuvent être rapidement étendus ou réduits et accessibles à tout moment et en tout lieu. L'informatique en nuage peut aider les assureurs à répondre rapidement aux besoins des clients et à s'adapter avec souplesse à l'évolution du marché et des technologies.

Le cloud computing : Son utilisation dans le secteur de l'assurance

Les assureurs ont fait un usage croissant de l'informatique en nuage ces dernières années.[4] Les services en nuage ont d'abord été appliqués aux fonctions de soutien commercial, telles que la gestion des clients ou les applications de collaboration. Aujourd'hui, le *cloud computing* est utilisé dans des fonctions commerciales essentielles, telles que le développement de produits, la distribution, la souscription ou la gestion des sinistres. Cela entraîne un certain nombre d'avantages et de risques pour le secteur des assurances.

Les avantages et les risques associés à l'informatique en nuage dépendront du modèle de déploiement et de service choisi.[5] En termes d'avantages, le *cloud computing* permet aux assureurs de partager des réseaux, des serveurs, du stockage, des applications et des services disponibles à la demande qui peuvent être rapidement étendus ou réduits et accessibles à tout moment et en tout lieu. Ainsi, le *cloud computing* permet aux assureurs de lancer rapidement de nouveaux produits et services, de rendre les processus commerciaux plus efficaces et de réduire les coûts des technologies de l'information (TI).

4 Voir L'étude de cas britannique ci-dessous.

5 Pour obtenir plus d'informations sur les différents types de modèles de cloud computing, voir les pages 5 à 9 du document Insights du FSI.

Les risques résultant de l'utilisation de services informatiques en nuage fournis par des tiers peuvent être différents des accords d'externalisation traditionnels. Ceci est attribuable aux caractéristiques uniques des dispositifs d'informatique en nuage, tels que :

- Les ressources informatiques partagées dans certains modèles de déploiement du cloud
- Les types d'informations stockées et traitées
- La répartition géographique des ressources informatiques et des fournisseurs
- Le petit nombre de fournisseurs mondiaux de services en nuage, ce qui entraîne une concentration du marché susceptible d'entraîner des conséquences systémiques. La nature transfrontalière des services en nuage complique la surveillance efficace de tous ces risques.

Le *cloud computing* : Approches en matière de réglementation et de surveillance

Le rapport de la FSI donne un aperçu des nouvelles approches en matière de réglementation et de surveillance de l'informatique en nuage dans le secteur des assurances, en s'appuyant sur des informations publiques et des entretiens menés auprès de 14 autorités financières situées en Asie, en Europe et en Amérique du Nord.

Approches en matière de réglementation et de surveillance

Il existe actuellement une série d'approches en matière de réglementation différentes adoptées par les 14[6] autorités de surveillance des assurances couvertes dans le présent rapport (Tableau 1). Celles-ci peuvent être divisés en quatre grandes catégories :

- **Application des règlements pertinents du cadre général d'externalisation à l'informatique en nuage.** Les autorités qui suivent cette approche comprennent les suivantes : APRA, BSIF, HKIA, IRDAI, SAMA, MAS, FINMA et la FCA. L'informatique en nuage est soit supposée relever de ces règlements, soit une section spécifique dans ces règlements est attribuée à l'informatique en nuage (comme par exemple MAS).

6 Australian Prudential Regulation Authority, Australie (APRA), Bureau du surintendant des institutions financières (BSIF) Canada, Autorité européenne des assurances et des pensions professionnelles (AEAPP), Union européenne, Autorité de Contrôle Prudentiel et de Résolution (ACPR) France, Federal Financial Supervisory Authority (BaFin) Allemagne, Insurance Authority, Hong Kong (HKIA), Insurance Regulatory and Development Authority of India (IRDAI) Inde, De Nederlandsche Bank (DNB) Pays-Bas, Saudi Arabian Monetary Authority (SAMA) Arabie Saoudite, Monetary Authority of Singapore (MAS) Singapour, Autorité suisse de surveillance des marchés financiers (FINMA) Suisse, Financial Conduct Authority (FCA) Royaume-Uni, Prudential Regulation Authority (PRA) Royaume-Uni, National Association of Insurance Commissioners (NAIC) États-Unis.

En général, les cadres d'externalisation sont basés sur les principes de haut niveau du Forum conjoint sur l'externalisation.[7]

- **Application des règlements pertinents du cadre de gouvernance et de gestion des risques à l'informatique en nuage.** Les autorités qui suivent cette approche comprennent celles qui appliquent la directive européenne Solvabilité II, où les dispositions relatives à l'externalisation font partie du cadre de gouvernance et de gestion des risques (AEAPP, ACPR, BaFin, DNB et PRA) ainsi que d'autres autorités ayant des réglementations en matière de gouvernance et de gestion des risques, telles que l'APRA, HKIA, IRDAI, FINMA et NAIC.
- **Application des règles pertinentes du cadre de sécurité de l'information à l'informatique en nuage.** Les autorités qui suivent cette approche comprennent les suivantes : APRA, BSIF, BaFin, IRDAI, SAMA, MAS et NAIC. Bien que ces réglementations soient généralement pertinentes pour l'utilisation de l'informatique dématérialisée, l'IRDAI, la SAMA et la MAS comprennent des articles propres aux exigences spécifiques à l'informatique dématérialisée. Les réglementations en matière de sécurité de l'information sont généralement basées sur les éléments fondamentaux de la cybersécurité pour le secteur financier du G7.[8]
- **Recommandations spécifiques au nuage ou attentes en matière de surveillance.** L'APRA, le BSIF, l'ACPR, la BaFin, la DNB et la FCA ont soit fourni des orientations/recommandations soit clarifié leurs attentes en matière de réglementation dans des circulaires, des notes de service, des documents sur les bonnes pratiques et d'autres documents publiés sur l'utilisation de l'informatique en nuage.
- **Application des règles pertinentes du cadre de sécurité de l'information à l'informatique en nuage.** Les autorités qui suivent cette approche comprennent les suivantes : APRA, BSIF, BaFin, IRDAI, SAMA, MAS et NAIC. Bien que ces réglementations soient généralement pertinentes pour l'utilisation de l'informatique dématérialisée, l'IRDAI, la SAMA et la MAS comprennent des articles propres aux exigences spécifiques à l'informatique dématérialisée. Les réglementations en matière de sécurité de l'information sont généralement basées sur les éléments fondamentaux de la cybersécurité pour le secteur financier du G7.[9]
- **Recommandations spécifiques au nuage ou attentes en matière de surveillance.** L'APRA, le BSIF, l'ACPR, la BaFin, la DNB et la FCA ont soit fourni des orientations/recommandations soit clarifié leurs attentes en matière de réglementation dans des circulaires, des notes de service, des documents sur les bonnes pratiques et d'autres documents publiés sur l'utilisation de l'informatique en nuage.

7 Le Forum conjoint a été créé sous l'égide du Comité de Bâle sur le contrôle bancaire (CBCB), de l'Organisation internationale des commissions de valeurs (OICV) et de l'Association internationale des contrôleurs d'assurance (AICA) pour traiter des questions communes aux secteurs de la banque, des valeurs mobilières et des assurances, et notamment la réglementation des conglomérats financiers. Les principes peuvent être consultés ici : https://www.bis.org/publ/joint12.htm

8 Consultable à l'adresse suivante : https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

9 Consultable à l'adresse suivante : https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Réglementation et déclaration de l'autorité de surveillance s'appliquant à l'externalisation vers le cloud

Cadres de référence	Externalisation		Gouvernance et gestion des risques		Sécurité des informations	
	Généralités	Spécifique au cloud	Généralités	Spécifique au cloud	Généralités	Spécifique au cloud
APRA					*	
BSIF						
AEAPP						
ACPR						
BaFin					*	
HKIA						
IRDAI						
DNB						
SAMA						
MAS						
FINMA						
FCA						
PRA						
NAIC						

* En cours de consultation

Remarque: Cadre général; Déclaration spécifique au cloud computing; Cadre général avec une rubrique spécifique au « cloud »

Tableau 1 : Approches en matière de réglementation du cloud computing

En ce qui concerne les domaines sur lesquels portent les exigences, les documents de surveillance actuels sur l'informatique en nuage portent principalement sur la gouvernance, l'évaluation des risques, la protection et la sécurité des données, la continuité des activités ainsi que les stratégies de sortie.[10] L'enquête menée auprès des 14 autorités a également révélé que les cadres réglementaires présentent un certain nombre d'exigences et d'attentes communes en matière de *cloud computing*. Les autorités se concentrent généralement sur :

- L'adéquation entre la sécurité des informations et la confidentialité des données
- La robustesse des capacités informatiques et des capacités en matière de cybersécurité des fournisseurs de services en nuage
- L'efficacité des capacités de récupération et de reprise
- L'adéquation des droits d'audit, c'est-à-dire l'accès de l'autorité de contrôle à la documentation et aux informations, et la possibilité de procéder à des contrôles sur place chez le fournisseur.

10 L'analyse complète est présentée dans le document FSI Insights. L'étude a affiné la liste de secteurs réglementaires relatifs à l'externalisation, à la gouvernance et à la gestion des risques, ainsi qu'à la sécurité des informations, et a comparé les exigences qui s'appliquent de manière générale et les exigences propres au nuage. Le rapport analyse les différents domaines réglementaires tels que l'importance relative, la gouvernance, la diligence raisonnable, l'évaluation des risques, la protection et la sécurité des données, la localisation, la sous-traitance, la continuité des activités et les stratégies de sortie, ainsi que le suivi, le contrôle, l'audit et l'accès.

Les autorités utilisent généralement des orientations non contraignantes sous forme de principes et de recommandations, en adoptant une approche proportionnée et adaptée à la taille, à la complexité ou au profil de risque des établissements financiers ou du service externalisé.

Surveillance de l'informatique en nuage

Les autorités adoptent des approches différentes afin de surveiller l'utilisation des services de *cloud computing* par les assureurs. La manière dont les assureurs sont tenus de communiquer leurs projets d'informatique dématérialisée à l'autorité de surveillance varie également, allant de la notification à la consultation, en passant par l'autorisation (Tableau 2).

	Notification	Consultation ou autorisation
APRA	Oui, pour les accords d'externalisation impliquant un nuage, les risques inhérents sont faibles.	Consultation, pour les accords d'externalisation impliquant des activités matérielles en cas de délocalisation et pour les accords impliquant des risques inhérents accrus ou extrêmes, qu'il y ait délocalisation ou non.
BSIF	Non	Non
AEAPP	Oui, pour les accords d'externalisation impliquant des fonctions critiques ou importantes.	Non
ACPR	Oui, pour les accords d'externalisation impliquant des fonctions critiques ou importantes.	Non
BaFin	Oui, pour les accords d'externalisation impliquant des fonctions critiques ou importantes.	Non
HKIA	Oui, pour les accords d'externalisation matérielle.	Non
IRDAI	Non	Non
DNB	Oui, pour les accords d'externalisation matérielle.	Une forme de consultation est nécessaire.
SAMA	Non	Autorisation, pour l'externalisation matérielle et pour tout accord de services en nuage.
MAS	Non	Non
FINMA	Non	Autorisation, pour les accords d'externalisation impliquant des fonctions importantes ou de contrôle en rapport avec le plan de développement.
FCA	Oui, pour les accords d'externalisation matérielle.	Non
PRA	YOui, pour les accords d'externalisation impliquant des fonctions critiques ou importantes	Non
NAIC	Non	Non

Tableau 2 : Communication des projets d'informatique en nuage

En général, le cloud computing est contrôlé dans le cadre des examens des risques opérationnels des assureurs, avec des vérifications sur place et hors site, et conformément à une approche fondée sur les risques. Les inspections sur site comprennent l'examen des éléments suivants :

- Documents justificatifs, par exemple la diligence raisonnable préalable et l'évaluation des risques de l'activité à externaliser, ainsi que le contrat d'externalisation lui-même
- Les processus de l'assureur en matière de gestion de la cybersécurité, de suivi des rapports et des contrôles, et de plans de continuité des activités

Les contrôles hors site se concentrent sur l'évaluation des pratiques de gouvernance et de gestion des risques de l'assureur, et comprennent :

- Dépôt de notification ou d'approbation envoyé aux autorités
- Informations publiques, par exemple les certifications et les rapports d'assurance d'un fournisseur de services en nuage
- Rapports réglementaires sur les activités d'externalisation, par exemple la politique d'externalisation d'un assureur, les évaluations des risques propres et de la solvabilité (ORSA), les rapports d'externalisation
- Examens thématiques et questionnaires spécifiques permettant d'obtenir des informations précises sur les activités de l'assureur en matière de *cloud computing*

Autres facteurs

Le rapport a permis de dégager un certain nombre de conclusions et de considérations essentielles pour les contrôleurs des assurances :

- Bien que le cloud computing soit souvent déjà soumis à des exigences générales d'externalisation, il est utile de clarifier les attentes réglementaires spécifiques au cloud afin de :
  - traiter les risques potentiels propres à l'informatique en nuage
  - fournir une garantir réglementaire en ce qui concerne l'utilisation des services en nuage
  - soutenir les acteurs du marché dans leur adoption responsable de la technologie
- Les cadres et exigences réglementaires qui en découleraient doivent idéalement être fondés sur des principes, neutres sur le plan technologique, cohérents entre les secteurs financiers et appliqués de manière proportionnée
- La coopération internationale entre les autorités d'origine et d'accueil, notamment en ce qui concerne le partage des informations pertinentes sur les fournisseurs de services en nuage, est particulièrement importante pour assurer une surveillance efficace des activités de l'informatique en nuage

Le rapport de la FSI n° 13, en anglais, et intitulé « Approches en matière de réglementation et de surveillance de l'informatique « en nuage » : approches prudentielles émergentes pour les compagnies d'assurance » (Crisanto, Donaldson, Garcia Ocampo et Prenio, 2018) peut être consulté directement ici.

ÉTUDE DE CAS : LE BRÉSIL

L'étude de cas sur le Brésil a été présentée par Paulo Miller et Gustavo Adolfo Araujo Caldas de la SUSEP, Brésil

Les assureurs sur le marché brésilien utilisent actuellement les services de cloud *computing* principalement pour soutenir des activités et des fonctions non essentielles telles que notamment les ressources humaines et les activités de gestion. Le marché compte un nombre croissant de sociétés InsurTech, ce qui pourrait accroître l'utilisation des services de *cloud computing* par les assureurs. Les principaux fournisseurs de services en nuage sur le marché brésilien sont Amazon, Microsoft et Google. Les principaux avantages de l'informatique dématérialisée ont été une plus grande évolutivité et, avec la numérisation croissante, un temps dédié aux entreprises afin qu'elles puissent se concentrer sur d'autres aspects de leur activité. L'un des principaux défis auxquels sont confrontés les prestataires a été la migration d'un prestataire de services vers un autre prestataire.

En matière de réglementation, la SUSEP en est aux premières étapes de la surveillance active du comportement et des tendances du marché ainsi que de l'engagement des acteurs du marché afin de déterminer s'il convient d'édicter une réglementation spécifique concernant l'utilisation de l'informatique en nuage.

Il n'existe actuellement aucun cadre réglementaire spécifique concernant l'utilisation du cloud computing dans le secteur des assurances au Brésil. Une résolution récemment publiée par la banque centrale sur la cybersécurité et les services en nuage (Res CMN n° 4.658/2018) sert actuellement de référence pour les services et activités d'externalisation en nuage sur le marché des assurances. Le règlement exige que les entités émettent des notifications à la banque centrale, laquelle dispose d'un droit de veto et peut imposer des exigences supplémentaires. La banque centrale permet aux entités de stocker leurs données dans des serveurs à l'étranger, sous réserve d'une exigence du contrat stipulant que la banque dispose d'un droit d'accès aux données. Tout comme le Règlement général sur la protection des données (RGPD), la confidentialité des données personnelles est d'une importance capitale.

Pour des questions ou plus d'informations sur les activités de la SUSEP,
veuillez contacter gustavo.caldas@susep.gov.br ou paulo.vianna@susep.gov.br

ÉTUDE DE CAS : ROYAUME-UNI

L'étude de cas britannique a été présentée par Sanjeev Chandran de la PRA, Banque d'Angleterre, Royaume-Uni

En 2019, la PRA a mené une enquête qui visait à identifier et à obtenir une vision plus large de l'utilisation des services de *cloud computing* par les assureurs au Royaume-Uni. L'enquête a été envoyée à 30 des plus grands assureurs et a révélé que :

- The use of cloud services among insurers is high (74 % of respondents), but still lL'utilisation des services en nuage par les assureurs est élevée (74 % des participants), mais reste inférieure à celle des banques
- La plupart des assureurs adoptent le modèle logiciel en tant que service (SaaS)
- Les fonctions critiques et sensibles sont en cours de migration vers le nuage
- Les principales fonctions que les assureurs externalisent vers le Cloud comprennent la gestion des opérations (16 %) et la gestion de la relation client (CRM) (16 %) (voir Figure 1 ci-dessous)

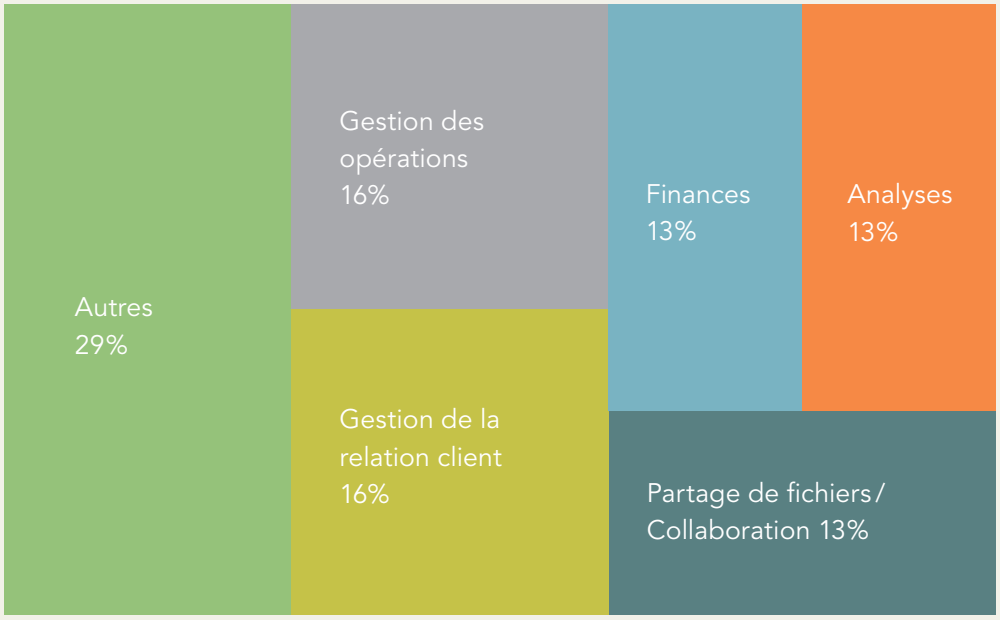

Figure 1 : Proportion des applications qui utilisent des services de cloud computing, ventilée par fonction (enquête PRA sur les nuages des assureurs, 2019)

En ce qui concerne l'utilisation des services en nuage dans le secteur financier, la réglementation de la PRA a mis l'accent sur le renforcement de la résilience opérationnelle des institutions financières. En règle générale, les assureurs britanniques sont tenus de notifier à la PRA tout accord d'externalisation matérielle. Cela comprend l'utilisation de l'informatique en nuage. Au fil du temps, des recommandations et des lignes directrices spécifiques pour les accords d'externalisation dans le nuage ont été émises pour

les entreprises de services financiers au Royaume-Uni, comme le résume le calendrier ci-dessous (voir la Figure 2 ci-dessous) :

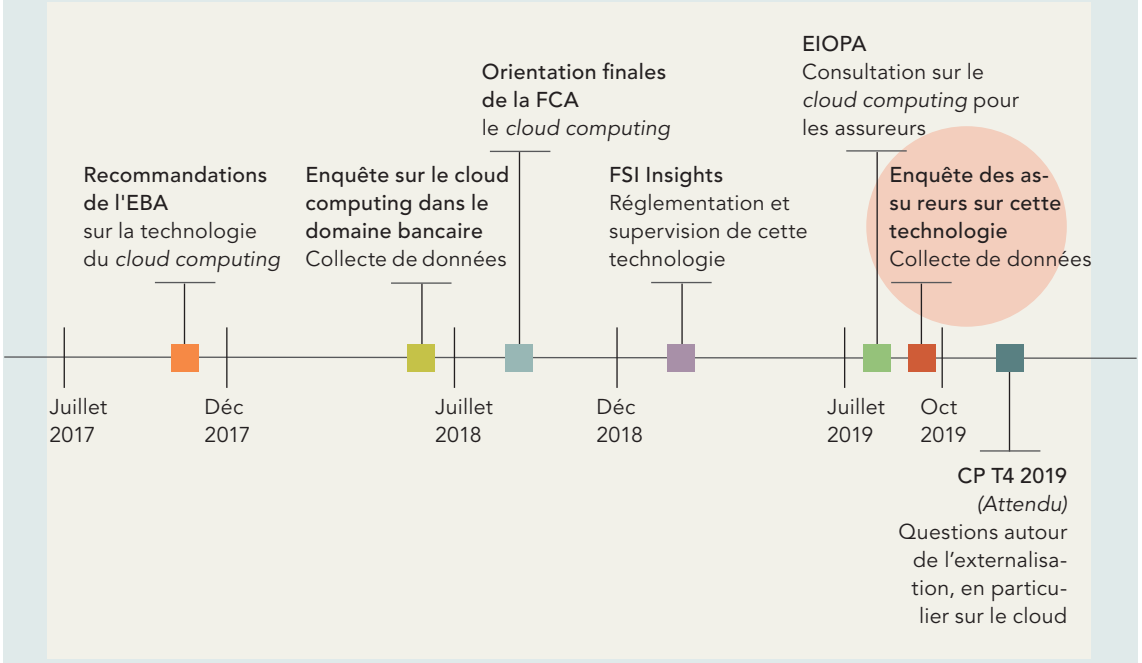

Figure 2 : Calendrier de l'établissement des recommandations et des lignes directrices pour les accords d'approvisionnement en matière de cloud computing au Royaume-Uni

L'un des principaux axes de l'approche réglementaire actuelle de la PRA consiste à s'appuyer sur la surveillance à l'échelle macro afin de renseigner la surveillance à l'échelle micro. À ce sujet, il convient de prendre en considération trois questions essentielles lorsqu'une entreprise migre ses fonctions vers le nuage :

- La gestion et la gouvernance de l'entreprise : quel est le modèle de responsabilité partagée de l'entreprise ?
- Où sont stockées les données et quelle est leur sécurité : quel est l'emplacement précis du fournisseur de services en nuage et qui est habilité à vérifier les données ?
- Risque de concentration des fournisseurs de services en nuage et facilité d'interchangeabilité : L'entreprise peut-elle facilement modifier son ou ses accords d'externalisation ? De quels pouvoirs de négociation l'assureur dispose-t-il ?

À l'avenir, la PRA continuera le développement de son approche de la surveillance à l'échelle micro de trois manières : aligner les approches de surveillance entre les secteurs de la banque et de l'assurance, veiller à ce que toutes les directives internationales soient respectées le cas échéant et, conformément à la surveillance fondée sur le risque, se concentrer sur les domaines susceptibles d'avoir un impact maximal.

Les principaux enseignements tirés jusqu'à présent sont les suivants :

- Il est primordial de considérer l'informatique dématérialisée dans le cadre plus large de la résilience opérationnelle.
- Il est nécessaire d'établir un « niveau de base » par rapport auquel les stratégies des entreprises en matière de *cloud computing* peuvent être évaluées. Les contrôleurs en sont actuellement au balbutiement de leur expérience avec le nuage.
- Il est important que les autorités de surveillance des assurances saisissent les relations entre les niveaux micro et macro. Cela signifie qu'il est nécessaire de tirer des enseignements des évaluations de chaque entreprise ainsi que des initiatives sectorielles.
- Il faut également tenir compte des facteurs externes au secteur. Au-delà de l'alignement sur le secteur bancaire, il peut être intéressant d'examiner comment les secteurs non financiers utilisent le « nuage ».
- Il est nécessaire d'assurer la cohérence des approches réglementaires entre les différentes juridictions.

Pour des questions ou plus d'informations sur les activités pertinentes de la PRA, veuillez contacter Sanjeev.Chandran@bankofengland.co.uk

ÉTUDE DE CAS : AEAPP

L'étude de cas de l'AEAPP a été présentée par Lázaro Cuesta Barberá de l'AEAPP

Cette étude de cas s'appuie sur le rapport de l'AEAPP intitulé « Externalisation vers le cloud : Contribution de l'AEAPP au plan d'action Fintech de la Commission européenne »(2019) 10 et Document de Consultation de l'AEAPP sur la proposition de lignes directrices sur l'externalisation des fournisseurs de services cloud » (2019).[11] Les résultats d'une enquête sur l'utilisation des services de nuage ont révélé que le recours au *cloud computing* est plus fréquent chez les nouveaux arrivants, dans quelques niches de marché et chez les grands assureurs. Dans le cadre de leurs stratégies plus larges de transformation numérique, de nombreux grands (ré)assureurs européens étendent leur utilisation du nuage. Le niveau d'utilisation n'est pas non plus homogène parmi les différents États membres de l'UE.

11 Consultable à l'adresse suivante : https://www.eiopa.europa.eu/content/consultation-proposal-guidelines-outsourcing-cloud-service-providers_en

Dans le cadre de Solvabilité II, l'utilisation du *cloud computing* par les assureurs[12] s'inscrit dans le cadre plus large de l'externalisation[13] au titre des Articles 38 et 49 de la directive Solvabilité II et de l'article 274 du règlement délégué Solvabilité II. Les lignes directrices de l'AEAPP sur le système de gouvernance fournissent également des orientations fondées sur des principes. Les règlements applicables portent principalement sur la gouvernance et la gestion des risques. Une disposition générale clé stipule que la responsabilité des activités et des fonctions externalisées doit rester au sein de l'assureur, et que les assureurs doivent appliquer une politique d'externalisation consignée par écrit. La directive Solvabilité II (Article 49, paragraphe 2) a également imposé certaines limites à l'externalisation des fonctions et activités opérationnelles critiques ou importantes. Ces activités ne doivent pas, entre autres, être entreprises d'une manière qui entraîne l'une des conséquences suivantes :

- Compromettre matériellement la qualité du système de gouvernance de l'assureur
- Augmenter indûment le risque opérationnel
- Compromettre la capacité des autorités de surveillance à contrôler le respect par l'assureur de ses obligations
- Mettre en péril le service continu et satisfaisant aux assurés

En termes d'exigences de surveillance, les entités d'assurance sont tenues de notifier à l'autorité de surveillance toute activité et tout développement importants, avant d'externaliser ces activités/fonctions ainsi que toutes les activités ultérieures. En outre, les organismes d'assurance sont tenus de disposer d'un accord d'externalisation écrit et d'informer les autorités de surveillance de son contenu, ainsi que des critères appliqués pour le choix du fournisseur de services en nuage.

Toutefois, certains secteurs réglementaires propres au *cloud computing* demandent encore à être clarifiés. Ces secteurs sont les suivants :

- Application de la définition réglementaire de l'externalisation à l'achat de services en nuage
- Évaluation des risques et de l'importance relative et notification aux autorités compétentes avant de conclure des accords d'externalisation dans le nuage
- Gestion des risques spécifiques liés à l'utilisation des services de *cloud computing* (par exemple, sécurité des données et des systèmes, confidentialité, risque juridique et de réputation, risque de concentration)

12 Toutes les références aux « assureurs » dans cette partie incluent également les réassureurs.

13 L'Article 13, paragraphe 28, de la directive Solvabilité II dispose que : « l'externalisation » est un accord de quelque forme que ce soit entre une entreprise d'assurance ou de réassurance et un prestataire de services, qu'il s'agisse ou non d'une entité contrôlée, en vertu duquel ce prestataire de services exécute un processus, un service ou une activité, directement ou par sous-traitance, qui serait autrement exécuté par l'entreprise d'assurance ou de réassurance elle-même.

- Application des exigences en matière d'audit et d'accès aux dispositifs de *cloud computing*
- Supervision des accords d'externalisation en matière de *cloud computing*

De juillet à septembre 2019, l'AEAPP a lancé une consultation publique sur la proposition de lignes directrices sur l'externalisation vers des fournisseurs de services dans le nuage.[14] Dans ce contexte, il convient de mentionner la ligne directrice sur la « Surveillance des accords d'externalisation dans les nuages par les autorités de surveillance », qui stipule que dans le cadre de leurs évaluations, les autorités de surveillance doivent évaluer les aspects suivants en utilisant une approche fondée sur le risque :

- Gouvernance des accords d'externalisation
- Disponibilité de ressources suffisantes, de compétences et de connaissances adéquates pour surveiller les activités d'externalisation vers le cloud
- Risques (comme par exemple, les risques opérationnels, de réputation, informatiques, stratégiques et de concentration) associés à l'externalisation vers le cloud

Il existe des dispositions particulières concernant les inspections sur place effectuées dans les locaux des fournisseurs de services en nuage. Les autorités de surveillance sont tenues de posséder les connaissances et l'expérience nécessaires pour contrôler ces exigences, c'est-à-dire des connaissances en matière de TI et de cybersécurité, de gestion de la continuité des activités, etc. Les autorités de surveillance peuvent prendre les mesures suivantes lorsque des problèmes sont identifiés : améliorer le dispositif de gouvernance, limiter ou restreindre la portée des fonctions externalisées ou exiger la sortie d'un ou plusieurs dispositifs d'externalisation.

Le projet de lignes directrices a pris en considération la contribution de l'AEAPP au plan d'action Fintech de la Commission européenne (mars 2019) et les recommandations de l'Autorité bancaire européenne (ABE) sur l'externalisation vers des fournisseurs de services en nuage. Ces lignes directrices doivent être adoptées en 2020.

Pour des questions ou plus d'informations sur les activités de L'AEAPP,
veuillez contacter Lazaro.Cuesta@eiopa.europa.eu

14 Consultable à l'adresse suivante :
https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers

Questions et débats

Comment les contrôleurs peuvent-ils procéder à des contrôles/inspections sur place lorsque le serveur en nuage est situé dans une autre juridiction, en particulier dans les pays sans accord de coopération ? Ce sujet est souvent abordé par les contrôleurs. L'inspection sur place représenterait un véritable défi pour les contrôleurs, car elle nécessite de nombreuses compétences et ressources. L'élément le plus important est que les contrôleurs disposent de droits d'audit sur les installations des fournisseurs de services en ligne. Dans la pratique, à la connaissance des experts de l'appel, en aucun cas les contrôleurs n'ont exercé ce droit. Il n'existe qu'un seul cas particulier où un contrôle sur place a eu lieu : au sein d'une juridiction, un fournisseur de services en nuage desservait 70 % du marché. Il y a également eu des questions techniques très spécifiques sur la sécurité que les contrôleurs devaient connaître. Dans tous les autres cas, cependant, les contrôleurs ont tenu des réunions au niveau local, dans leur juridiction, avec le fournisseur de services en nuage afin de comprendre les accords et les conditions de l'accord d'externalisation. Chaque accord est différent, et il est important de comprendre les caractéristiques propres à chaque contrat. En règle générale, l'utilisation du nuage n'en est qu'à ses balbutiements et les bonnes pratiques apparaîtront de plus en plus clairement au fil du temps.

Lors de la conférence annuelle de l'AICA de 2019, un important fournisseur de services en nuage a exprimé son souhait de participer davantage aux discussions de contrôle concernant la réglementation du nuage. Qu'en pensez-vous ? Il est important que les contrôleurs maintiennent un contact et un dialogue constant avec les fournisseurs de services en nuage. Les contrôleurs doivent comprendre le fonctionnement des fournisseurs de services en nuage, les caractéristiques des services fournis et les implications en matière de sécurité pour l'assureur. Les fournisseurs de services dans le nuage doivent également comprendre les autorités de surveillance, les risques que celles-ci perçoivent de leur point de vue et les exigences réglementaires respectives. À ce titre, il serait utile que les contrôleurs et les fournisseurs de services en nuage disposent d'une ligne de communication directe et se comprennent mutuellement.

Si l'informatique en nuage est un accord d'externalisation, pourquoi devrait-il y avoir une obligation de notification spéciale au contrôleur, au lieu d'être traité comme toute autre fonction d'externalisation ? Au titre de la directive Solvabilité II, les assureurs sont au moins tenus d'informer l'autorité de surveillance dans tous les cas où des fonctions essentielles sont externalisées, et cela s'applique également à l'externalisation dans le nuage. La personnalisation réside dans le contenu et les informations requises dans la notification, là où les autorités de surveillance peuvent demander des informations spécifiques propres aux caractéristiques de l'informatique en nuage. Ces informations uniques qu'il peut être utile de clarifier pour les contrôleurs comprennent, par exemple, l'utilisation, les types et le stockage des données concernées par l'accord sur le *cloud computing*.

Quelles sont les bonnes pratiques ou les leçons à tirer jusqu'à présent, telles que ce « qu'il faut faire et ne pas faire » ? L'utilisation du nuage pour des fonctions critiques n'en est qu'à ses débuts, mais il serait bon que les autorités de surveillance disposent de rapports réglementaires solides sur les dispositions relatives à l'informatique dématérialisée afin d'obtenir des informations détaillées qu'elles pourront utiliser pour évaluer si les assureurs gèrent correctement les risques liés à l'utilisation du cloud. Les autorités de contrôle ne doivent pas se hâter de réglementer avant avoir évalué le statut des services de *cloud computing* sur leurs marchés. Il

est important que les autorités de surveillance évaluent si et comment le *cloud computing* est utilisé sur leur marché afin d'identifier les moyens de le réglementer. Le SUSEP a fait part de son approche jusqu'à présent, consistant à s'aligner en grande partie sur le secteur bancaire, et s'attache pour l'instant à garantir dans le contrat que les contrôleurs doivent avoir accès aux données et à la confidentialité des données personnelles.

L'Initiative est un partenariat entre :

Soutenu par :

Hébergée par :

Initiative Accès à l'assurance
Hébergée par le Projet Financial Systems
Approaches to Insurance de la GIZ
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Téléphone : +49 61 96 79-1362
Fax : +49 61 96 79-80 1362
E-mail : secretariat@a2ii.org
Site web : www.a2ii.org

a2ii_org

Promouvoir l'accès pour tous à une assurance responsable et inclusive.