ACP Autorité de Contrôle Prudentiel
Banque de France

Analyses et Syntheses

Les risques associés au *Cloud computing*

n°16 – juillet 2013

Sommaire

1. Caractéristiques du *Cloud computing* **5**

1.1. Éléments de définition 5

1.2. Précisions apportées aux critères de définition 6

1.3. Distinction entre *Cloud computing* et infogérance classique 6

2. Mise en œuvre de services de *Cloud computing* **7**

2.1. Enjeu économique 7

2.2. Avantages attendus 7

2.3. Risques perceptibles pour les secteurs de la banque et de l'assurance 8

2.4. Usage fréquent pour les domaines de gestion et de support informatique 9

2.5. Décision d'engagement dans une prestation de *Cloud computing* 9

3. Mesures d'accompagnement requises **10**

4. Adéquation de l'environnement réglementaire **11**

5. Principaux enseignements et bonnes pratiques pouvant être dégagés **11**

Annexe : Enquête relative au *Cloud Computing* (questionnaire envoyé) **15**

Objectif de l'enquête 15

1. Caractéristiques du cloud computing 15

2. Les cas d'usage du « cloud computing » 16

3. L'environnement juridique du « cloud computing » 16

4. Les risques et les mesures de sécurité associés au cloud computing 16

Les risques associés au *Cloud computing*

Résumé :

Les systèmes d'information sont un enjeu stratégique, aussi bien dans le secteur bancaire que dans le domaine des assurances. Parmi les évolutions récentes, le développement du *Cloud computing* est devenu un sujet d'attention.

Le *Cloud computing* (aussi appelé informatique « en nuage » ou informatique « nébuleuse ») est défini[1] comme un « mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients ».

Ce sujet est d'actualité pour de nombreuses instances de régulation. En France, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) travaille à un encadrement via un dispositif de certification. La Commission Nationale de l'Informatique et des Libertés (CNIL) a publié en 2012 des recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud computing*. À l'étranger, plusieurs autorités de contrôle ont émis des avis (États-Unis, Singapour, Pays-Bas), voire imposé un système d'autorisation préalable (Espagne) pour l'utilisation de cette technologie.

Dans ce contexte, le Secrétariat général de l'Autorité de contrôle prudentiel (SGACP) a souhaité, au travers d'une courte enquête, engager un dialogue avec les entreprises des secteurs de la banque et de l'assurance sur le périmètre, l'usage et les risques du *Cloud computing*. Quatorze entreprises du secteur de l'assurance et douze du secteur de la banque ont répondu à un questionnaire au début de cette année, donnant ainsi une vue représentative sur ces sujets.

Au terme de ces échanges, il est d'abord apparu utile de préciser la notion de *Cloud computing* en proposant une définition multicritère fondée sur celle du *National Institute of Standards and Technology* (NIST). Le SGACP propose donc de caractériser ces prestations de la façon suivante : le *Cloud computing* consiste à déporter sur des serveurs distants des données et des traitements informatiques traditionnellement localisées sur des serveurs locaux, voire sur le poste de l'utilisateur ; il permet l'accès via le réseau, à la demande et en libre service, à des ressources informatiques virtualisées et mutualisées généralement facturées à l'usage ; trois types de services sont proposés (IaaS – *Infrastructure as a Service*, PaaS – *Platform as a service*, SaaS – *Software as a Service*), déployés selon quatre modèles (*Cloud privé interne*, *Cloud privé externe* ou *Cloud communautaire*, *Cloud public*, *Cloud hybride*).

Les établissements de crédit et organismes d'assurance (entreprises) ayant répondu au questionnaire ont confirmé que le *Cloud computing* présente des risques supérieurs à l'infogérance classique. Les risques identifiés sont nombreux et couvrent la confidentialité des données, la disponibilité des données et traitements, l'intégrité (en particulier le risque de réversibilité ou enfermement) et enfin le domaine de la preuve et du contrôle. Ils s'accordent sur la nécessité d'un environnement juridique renforcé, certaines mesures techniques de sécurité, la nécessité de contrôler le prestataire, l'engagement du prestataire sur la continuité du service et, enfin, la nécessité d'obtenir une garantie du prestataire sur la réversibilité de la prestation.

En revanche, les avis divergent sur l'importance de l'enjeu économique autour des services de *Cloud computing*, nombre d'entreprises faisant valoir que les considérations de sécurité devaient l'emporter dans l'analyse de l'intérêt de telles prestations. Au demeurant, on constate qu'une grande majorité des entreprises utilisent le *Cloud computing* dans les domaines de gestion considérés comme hors « cœur de métier », même si un usage pour des domaines plus sensibles se fait également jour. Il semble également que les modalités d'adoption du *Cloud computing* soient différentes dans le domaine de l'assurance et de la banque.

À l'issue de cette première analyse, qui devra être affinée au fil des évolutions constatées dans l'usage et les risques du *Cloud computing*, l'ACP encourage les entreprises qu'elle contrôle à prendre des mesures de maîtrise des risques adaptées sur les points suivants :

[1] Vocabulaire de l'informatique et de l'internet, publié au JORF n° 129 du 6 juin 2010

- Juridique : par un encadrement contractuel impératif des prestations de *Cloud computing ;*

- Technique : avec le chiffrement lors du transport et du stockage des données (en l'absence d'anonymisation) ;

- Contrôle du prestataire : avec notamment la capacité d'audit et le droit de le faire pour l'ACP ;

- Continuité de la prestation : en veillant à ce que les contrats de service permettent de formaliser les attentes de l'entreprise cliente ;

- Réversibilité de la prestation : les conditions de réversibilité devant être prises en compte lors de la souscription du service ;

- Intégration et urbanisme du système d'information : l'organisation et la gouvernance des systèmes d'information devant être adaptés à l'utilisation du *Cloud computing*.

Ces bonnes pratiques s'inscrivent dans le cadre plus large défini pour le contrôle des prestations externalisées, y compris l'infogérance classique. Les attentes de l'ACP en termes de gouvernance des décisions, d'analyse des risques, de contractualisation, de pilotage et de contrôle interne des prestations de *Cloud computing* sont donc similaires à celles qui prévalent aujourd'hui dans le contrôle prudentiel.

Étude réalisée :

- Pour le SGACP, par Marc Andries (délégation au contrôle sur place), Guillaume Cassin (direction du contrôle des établissements mutualistes et entreprises d'investissement), Ayoub Bahhaouy, François Philippe et Yannick Foratier (direction des contrôles spécialisés et transversaux) ;

- Pour l'Organisation et Information de la Banque de France, par Andres Lopez Vernaza et Franck Rigodanzo.

LES RISQUES ASSOCIÉS AU *CLOUD COMPUTING*

Les systèmes d'information sont un élément stratégique du bon fonctionnement et de la stabilité des secteurs de la banque et de l'assurance. C'est aussi un domaine en évolution constante, sous l'effet du renouvellement des techniques et des offres de solution.

Parmi les évolutions récentes, le développement d'une nouvelle forme de gérance de l'informatique, le *Cloud computing* (« informatique en nuage »), est devenu un sujet d'attention pour l'Autorité de contrôle prudentiel (ACP).

Ce type de service consiste à déporter chez un prestataire le traitement de masse de données et/ou logiciels et à y accéder par un réseau comme Internet. En France, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), a abordé le *Cloud computing* dans son *Guide pour l'externalisation* (2010) et travaille à un encadrement du *Cloud* via un dispositif de certification. La Commission Nationale de l'Informatique et des Libertés (CNIL) a publié en 2012 des recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud computing*. Dans le secteur financier à l'étranger, la *Federal Financial Institutions Examination Council* a publié un avis (« *Statement* ») en juillet 2012. La *Monetary Authority of Singapore* a mis à jour ses *Technology Risk Management Guidelines* en juin 2012 pour y intégrer le *Cloud computing*. En Europe, la *Banco d'España* et la *De Nederlandsche Bank* ont publié leurs positions sur le *Cloud computing*.

Dans ce contexte, le Secrétariat général de l'Autorité de contrôle prudentiel (SGACP) a souhaité, avec une courte enquête, engager un dialogue avec les entreprises des secteurs de la banque et de l'assurance (entreprises) sur le périmètre du *Cloud computing*, la mesure des engagements dans ce type de solutions, l'appréciation des risques et les politiques de sécurité adoptées, tout comme l'adéquation et les textes réglementaires existants. Quatorze entreprises du secteur de l'assurance et douze du secteur de la banque ont répondu à cette enquête, donnant ainsi une vue représentative sur ces sujets.

La présente étude restitue à la profession les réponses apportées à l'enquête transmise sous la forme d'un questionnaire (cf. annexe). Elle formule un certain nombre de bonnes pratiques dont le SGACP examinera la mise en œuvre, tout en suivant avec attention les développements des risques associés au *Cloud computing.*

1. Caractéristiques du *Cloud computing*

1.1. Éléments de définition

L'expression *Cloud computing* recouvre différents types de services, susceptibles de continuer à évoluer dans le temps avec l'apparition de nouvelles solutions techniques. Pour éviter d'être contraint par un cadre pouvant rapidement devenir obsolète, le SGACP a choisi une définition s'appuyant sur la combinaison de différents critères, dont ceux proposés par le *National Institute of Standards and Technology* américain (NIST). Les entreprises interrogées ont confirmé qu'elles partageaient les éléments de définition ainsi proposés.

Cette définition, rappelée ci-dessous, distingue le concept général du *Cloud computing,* les types de service proposés, et les différents modèles de relation entre l'entreprise cliente et le prestataire :

- **Concept** : le *Cloud computing* consiste à déporter sur des serveurs distants des données et des traitements informatiques traditionnellement localisés sur des serveurs locaux, voire sur le poste de l'utilisateur. Il permet l'accès via un réseau, généralement entendu comme Internet, à la demande et en libre service, à des ressources informatiques virtualisées et mutualisées habituellement facturées à l'usage.

- **Services** : le *Cloud computing* fournit dans ses déclinaisons les plus courantes trois types de ressources.

  - L'IaaS (*Infrastructure as a Service*) offre une infrastructure informatique comme de la puissance de calcul, des machines virtuelles incluant un système d'exploitation, du stockage, des services de sauvegarde.

  - Le PaaS (*Platform as a Service*) fournit une plateforme de développement et/ou d'exécution intégrée, reposant sur un catalogue de composants logiciels et techniques standardisés dont l'infrastructure sous-jacente est transparente pour l'utilisateur.

  - Le SaaS (*Software as a Service*) est une solution applicative répondant à un domaine d'utilisation précis supportant une fonction métier (gestion de la relation clientèle, gestion financière, …) ou un service transverse (messagerie, outils collaboratifs, …).

- **Modèles** : le *Cloud computing* est déployé selon quatre modèles :

  - Les *clouds* privés internes sont gérés au sein de l'entreprise pour ses besoins et sur des infrastructures lui appartenant.

  - Les *clouds* privés externes sont dédiés aux besoins d'une seule entreprise ou d'un groupe d'entreprise mais hébergés chez un prestataire.

  - Les *clouds* publics sont gérés par une entreprise spécialisée qui loue ses services à de nombreuses entreprises. Le mot « public » renvoie ici à l'acception généralement utilisée par les acteurs du *Cloud computing*, c'est-à-dire un environnement ouvert et multi-clients.

  - Enfin, les *clouds* hybrides combinent de manière dynamique les *clouds* publics et privés.

Le *cloud* public est une forme particulière de gérance de l'informatique, pour laquelle la prestation est mutualisée pour un grand nombre de clients, et l'emplacement des données dans le « nuage » n'est généralement par porté à la connaissance des clients.

L'ACP est évidemment principalement attentive aux développements de prestations pour les banques et assurances sous la forme de *clouds* publics ou hybrides : en effet, ceux-ci mutualisent les services offerts à l'ensemble de leurs clients et/ou à leurs utilisateurs internes, créant un risque de perméabilité des données entre les différents bénéficiaires Mais il en va de même pour tout modèle de *cloud* privé externe dans lequel il existerait une mutualisation du service fourni à une entreprise contrôlée par l'ACP avec ceux proposés à d'autres clients, même des secteurs de la banque et de l'assurance, comme par exemple dans les *clouds* dits « communautaires », qui partagent des ressources entre un nombre limité de partenaires.

1.2. Précisions apportées aux critères de définition

Tout en validant les éléments de définition proposés par le SGACP, certaines entreprises ont souhaité les compléter par quelques précisions concernant les caractéristiques propres du *Cloud computing*.

La mutualisation de ressources géographiquement dispersées. Les grands groupes internationaux, tant dans le secteur de l'assurance que de la banque, identifient le *Cloud computing* comme un moyen de mutualiser fortement leurs ressources sans développements spécifiques. Le déploiement multi-pays et multi-entités en serait grandement simplifié. Un grand bancassureur international indique en outre que cette pratique permet la répartition des données sur des centres informatiques dispersés géographiquement ainsi que la disponibilité, en support, de nombreux personnels également dispersés géographiquement.

Une plus grande adaptabilité des ressources. Un groupe bancaire insiste sur la notion d'élasticité du service et sur le fait que le *Cloud computing* permet de disposer automatiquement des ressources informatiques demandées. Un groupe d'assurance considère même que l'adaptabilité en temps-réel du système d'information grâce au *Cloud computing* est une caractéristique majeure. À noter que la notion de libre service, qui permet de minimiser les interactions entre le client et le fournisseur dans la mise à disposition dudit service (offres prêtes à l'emploi selon des niveaux de services), n'est pas adoptée par tous : un groupe d'assurance considère que ce terme n'est pas totalement approprié car l'utilisation du *Cloud computing* nécessite la signature préalable d'un contrat.

La multiplication des définitions du *Cloud computing* montrerait selon une entreprise que la notion n'est pas encore stabilisée, notamment concernant la caractéristique « fragmentation des données ».

1.3. Distinction entre *Cloud computing* et infogérance classique

Une grande majorité des entreprises considère que le *Cloud computing* est un mode particulier d'externalisation de l'informatique et qu'il présente donc avec l'infogérance classique de nombreux caractéristiques et risques communs. Un grand groupe bancaire avance même que les exigences des banques vis-à-vis du *Cloud computing* peuvent ramener *de facto* les prestations de ce type à une infogérance classique.

Toutefois, l'opinion très majoritairement partagée avec le SGACP est que le *Cloud computing* présente des caractéristiques de risque supérieures à l'infogérance classique.

Parmi les caractéristiques spécifiques, la souplesse de dimensionnement et d'utilisation beaucoup plus élevée (matérialisée notamment par la facturation à l'usage) que dans l'infogérance classique est souvent mise en exergue. En contrepartie, le *Cloud computing* signe une perte d'influence de la part des entreprises clientes vis-à-vis des prestataires informatiques :

- d'une part, les acteurs du *Cloud computing* ne s'engagent que rarement sur des résultats mais préfèrent recourir à une obligation de moyens, la faiblesse voire l'absence de conventions de service (en anglais SLA « service level agreement ») dans le monde de l'informatique en nuage en étant un marqueur flagrant,

- d'autre part, une perte de flexibilité dans la construction de l'offre de service est mise en avant : là où l'infogérance permet d'obtenir une réponse sur mesure aux attentes exprimées, le *Cloud computing* ne propose, au moins pour l'instant, que des offres génériques,

- enfin, la crainte d'une perte de contrôle partielle du système d'information est clairement exprimée, que ce soit dans la maîtrise des données (localisation et résilience du service inconnues) ou dans leur dépendance à l'égard des prestataires. Ainsi, le maintien en conditions opérationnelles est désormais systématiquement effectué par le prestataire pour les services de *Cloud computing :* les tâches de pilotage des évolutions, recettes et règles de planification sont à la charge du fournisseur, de même pour la réalisation des montées de version, qui sont parfois réalisées sans même en informer les organismes clients.

2. Mise en œuvre de services de *Cloud computing*

2.1. Enjeu économique

Le SGACP a souhaité mesurer le niveau d'appétence vis-à-vis de ces services, notamment en raison d'un éventuel enjeu économique sur lequel les points de vue paraissent partagés.

Certains reconnaissent les réductions de coût (notamment par la facturation à l'usage) et des délais de mise en œuvre, tout en alertant sur les coûts cachés qui au final peuvent réduire cet avantage. Un groupe bancaire international signale également que le *Cloud computing* peut faciliter les échanges entre partenaires, par exemple pour des services comme la synchronisation des opérations d'export (*workflow* de crédit documentaire). Une autre entreprise espère un allègement des coûts d'infrastructures et de mise en œuvre ainsi qu'une facilité de gestion de son plan de continuité d'activité.

Sans nier ces avantages économiques théoriques, d'autres considèrent que ce sont les risques associés aux pratiques de *Cloud computing* qui doivent guider la décision d'y recourir ou non.

2.2. Avantages attendus

Des solutions plus souples. La rapidité de mise en œuvre, la facilité de gestion, la flexibilité et l'élasticité des solutions de *Cloud computing* sont les principaux éléments mis en avant. Certains soulignent la disponibilité, les performances, la grande accessibilité et la mobilité accrue des solutions de *Cloud computing* puisqu'une simple connexion Internet suffit. Les solutions *cloud* seraient ainsi avantageuses dans les domaines nécessitant une forte puissance de calcul sur des périodes ponctuelles, tant du côté de l'assurance et de la réassurance (modélisation et tarification) que pour la banque de marché (calculs de risque). Un assureur cite la réalisation de développements informatiques ayant une durée de vie limitée comme potentiellement dans la cible du *Cloud computing* au regard des délais de mise en œuvre requis. Quelques uns indiquent toutefois que cette souplesse est encore limitée : les offres de *Cloud computing* seraient pour l'instant prévues pour rester standardisées, voire ne seraient pas encore bien définies ou matures, les retours d'expérience étant encore peu nombreux.

Un meilleur accès aux technologies de pointe. Les solutions de *Cloud computing* sont souvent associées aux dernières technologies fondées sur des éléments standards et interopérables. Les entreprises qui considèrent qu'elles n'ont pas la taille critique, les ressources ou les expertises nécessaires y voient la possibilité de disposer d'un environnement en permanence conforme à l'état de l'art et aux exigences des clients et régulateurs. Pour une petite banque, le *Cloud computing* permet d'utiliser des centres informatiques récents et disposant d'une bonne performance énergétique. Concernant les applications offertes dans le *Cloud computing*, un certain nombre d'entreprises espèrent bénéficier des dernières fonctionnalités et des dernières mises à jour mais aussi d'une meilleure cohérence des fonctionnalités grâce à la mutualisation et à la centralisation. Un grand groupe international (banque et assurance) considère toutefois que l'intérêt du *Cloud computing* est limité aux services « utilitaires » et à faible niveau de risque et que cela s'apparente à des solutions « sur étagère ».

Une diminution des coûts informatiques. Le *Cloud computing* présenterait aussi un avantage en termes de coût, notamment grâce au paiement à l'usage et la facturation en coûts complets. Plus largement, certains annoncent une évolution du modèle économique et une baisse des investissements, considérées comme un avantage par les entreprises ayant des contraintes budgétaires fortes sur les investissements mais moindres sur les budgets de fonctionnement. Un grand bancassureur

international voit dans le *Cloud computing* la possibilité de dégager l'informatique interne d'un certain nombre de charges de développement et d'exploitation à faible valeur ajoutée afin de concentrer ses ressources sur les besoins à plus forte valeur ajoutée. Un autre y voit la possibilité d'alléger ses charges de gestion d'infrastructures.

L'argument de l'avantage financier doit toutefois être relativisé. En effet, en sens inverse, sont mis en avant les coûts cachés des solutions de *Cloud computing,* en raison des difficultés à interfacer et à intégrer le service souscrit avec l'infrastructure informatique de l'entreprise, ainsi que les impacts en termes de ressources humaines et processus des solutions SaaS.

L'avantage supposément conféré par le *Cloud* n'est toutefois pas unanimement apprécié : un grand établissement bancaire et un organisme d'assurance ne voient dans le *Cloud computing* aucun intérêt.

2.3. Risques perceptibles pour les secteurs de la banque et de l'assurance

Les entreprises se sont tous montrées sensibles, à des degrés divers toutefois, aux risques spécifiques générés par l'utilisation du *Cloud computing*. Ces risques constituent autant de freins à l'utilisation de cette technologie, particulièrement dans le cas des *Clouds* publics ou hybrides. Le principal obstacle semble prendre sa source dans la très faible marge de négociation lors de la contractualisation de l'offre de service, majoritairement générique. Ainsi, les organismes peinent à obtenir des aménagements spécifiques corrigeant les risques qu'ils ont identifiés.

Le **risque d'atteinte à la confidentialité des données** est celui qui est très majoritairement mis en avant. La faiblesse des offres de sécurité (notamment le chiffrement à la volée et la gestion des clés cryptographiques) est généralement citée en premier. L'absence de connaissance de la localisation des données ou le droit d'accès aux données au profit de certains États[2] est considérée comme un risque réglementaire fort : il est difficile de s'assurer de la conformité aux exigences réglementaires, telles que celles résultant de la réglementation en matière de secret bancaire et de protection des données personnelles et plus largement en matière de propriété intellectuelle, au sein d'une infrastructure mutualisée et potentiellement accessible par les régulateurs locaux. Ce risque serait encore accru en-dehors de l'Union Européenne. Un grand groupe international y voit même un risque de souveraineté (si les données et traitements des entreprises françaises n'étaient plus situés en France). La difficulté à maîtriser la sécurité des données sur toute la chaîne, compte tenu du nombre de parties prenantes susceptibles d'intervenir dans le cadre de l'exécution de la prestation, est également relevée. Il en est de même de la difficulté à s'assurer que le prestataire ne peut pas lire des données confidentielles à travers les journaux d'évènements de ses systèmes. Les difficultés d'intégration avec le système d'information de l'entreprise et le risque de multiplication des *clouds* interfacés avec le système d'information sont également signalés comme des obstacles potentiels ; une banque considère même que l'interconnexion entre son système d'information et celui du prestataire de *Cloud computing* peut créer une brèche de sécurité. Enfin, un autre groupe bancaire pointe la difficulté de s'assurer que le prestataire a détruit les données en cas d'arrêt de la prestation.

L'indisponibilité des données et des traitements est un autre risque généralement mentionné, avec une distinction entre la nécessaire continuité des services et la notion de disponibilité des services privilégiée par les fournisseurs de *Cloud computing*. Une entreprise précise que le fournisseur s'engage sur un taux de disponibilité mais que son non-respect n'est sanctionné que par des pénalités financières. Des groupes d'assurance voient en outre dans l'enchevêtrement des prestataires un risque pour l'identification du responsable du service et donc une fragilisation du SLA. Plusieurs entreprises indiquent au demeurant que l'engagement contractuel du prestataire de *Cloud computing* sur la disponibilité du service doit être relativisé puisque celui-ci ne peut garantir la puissance, voire la disponibilité dans certaines circonstances, du réseau Internet, qui est pourtant un élément clé pour la disponibilité des applications.

La perte d'intégrité, qu'elle touche les données ou les traitements, n'est pas citée explicitement mais transparaît dans les réponses. Certains craignent pour l'intégrité globale de leur système d'information en raison d'une perte d'expertise technique, voire d'une dépendance à un fournisseur. Enfin, le risque de non-réversibilité ou d'enfermement (*lock-in*) est perçu comme important, notamment dans la mesure où il est difficile d'évaluer la capacité du prestataire à

[2] Le cas du *Patriot Act* des Etats-Unis d'Amérique est souvent cité en exemple. Il permet aux services de sécurité américains d'accéder à des données à caractère personnel sur leur territoire ou à l'étranger si elles sont détenues par des sociétés américaines. Par ailleurs, un rapport récent du parlement européen (2012) indique que la loi FISAA *(« Foreign Intelligence Surveillance Amendments Act »),* spécifiquement ciblée sur les données de personnes non américaines situées à l'extérieur des Etats-Unis, est susceptible de donner un droit d'accès aux agences gouvernementales américaines à toutes les données stockées dans le nuage.

restituer les données dans un format exploitable. Un groupe bancaire précise qu'il sera difficile de ré-internaliser une prestation si les outils et formats du prestataire sont propres à ce dernier.

Les **faiblesses du *Cloud computing* dans le domaine du contrôle et de la preuve** sont également identifiées par un grand nombre. Est mise en avant la difficulté à auditer un prestataire, voire à en obtenir un droit d'audit, en raison de la multiplication des intervenants et de leur localisation géographique. Plus globalement, la difficulté à mettre en place un dispositif de contrôle interne adéquat est soulignée par un grand bancassureur international. Des groupes d'assurance constatent l'accroissement des risques de non-conformité, en raison notamment de la localisation des données et de l'identification de la loi applicable.

Même si ce type de prestation présente donc des risques particuliers, la très grande majorité des entreprises a précisé utiliser les méthodes d'analyse de risques habituelles pour l'analyse des solutions de *Cloud computing*. Certains ont toutefois complété leur méthodologie avec des scénarios de risques propres au *Cloud computing*. Un grand groupe bancaire considère par exemple qu'un risque d'architecture est intrinsèque au *Cloud computing* en raison de son intégration au système d'information de l'entreprise. Dans le même ordre d'idée, un autre émet l'idée qu'en raison de la mutualisation, l'exploitation d'une faille de sécurité sur un client pourrait impacter les autres clients hébergés chez le fournisseur.

A contrario, un petit établissement bancaire a précisé que le *Cloud computing* pouvait lui permettre d'accéder à un niveau de sécurité supérieur à celui qu'il pourrait mettre en œuvre lui-même.

2.4. Usage fréquent pour les domaines de gestion et de support informatique

Le niveau d'utilisation des solutions de *Cloud computing* est finalement cohérent avec les avantages et inconvénients soulignés. Ces solutions, d'ores et déjà couramment utilisées[3], sont toutefois pour l'instant réservées à des activités support, même si certaines sociétés sont prêtes à en faire un usage plus large.

En très grande majorité, le *Cloud computing* est utilisé dans des domaines de gestion considérés comme hors du « cœur de métier », sans qu'il soit toutefois donné de définition à cette expression, comme la gestion des ressources humaines, les finances (notes de frais), les achats ou la communication externe ou interne (réseaux sociaux d'entreprise, messagerie, calendrier, web conférence, partage de documents). Des grands groupes d'assurance précisent que les applications qui peuvent constituer un avantage concurrentiel n'ont pas vocation à être positionnées dans le *cloud*. D'autres entreprises disent recourir au *Cloud computing* selon la confidentialité et la localisation des données, tout en reconnaissant ne pas avoir d'assurance du respect de la confidentialité des données notamment hors d'Europe.

Toutefois, un usage pour des domaines plus sensibles se fait également jour. Un assureur indique utiliser une solution SaaS hybride pour sa comptabilité alors qu'un autre héberge dans le *cloud* des données de conformité réglementaire, comptables, financières, de trésorerie et d'investissement. Plusieurs grands groupes bancaires utilisent des services de *Cloud computing* dans le domaine de la gestion de la relation clientèle de la banque de détail, de la banque de financement et d'investissement et des services financiers. Un groupe bancaire déclare recourir au *Cloud computing* en matière de prescription immobilière. D'autres grands groupes font appel au *Cloud computing* pour des prestations d'hébergement de sites Internet institutionnels, voire pour des prestations liées à la sécurité informatique (filtrage des accès Internet). Certains assureurs indiquent ne pas s'interdire de répondre à des besoins d'infrastructure à des fins de développement ou de test (phase projet) par des solutions de *Cloud computing*.

2.5. Décision d'engagement dans une prestation de *Cloud computing*

Les modalités d'adoption du *Cloud computing* semblent différentes dans le domaine de l'assurance et de la banque.

Le choix de recourir au *Cloud computing* en assurance impliquerait, dans la très grande majorité des cas, la direction générale ou le comité de direction. L'adoption du *Cloud computing* sur des données sensibles ou « cœur de métier » nécessiterait également une validation de la direction générale. Un autre assureur indique que cette décision serait du ressort de sa direction des systèmes d'information (DSI).

Du coté bancaire, le processus d'adoption du *Cloud computing* suit les processus d'évolution du système d'information avec une initiative des métiers ou fonctions support et un pilotage du projet par la DSI après analyse de risques. Dans

[3] Environ la moitié des entreprises d'assurance ayant répondu utilisent une solution *Cloud*, dont les deux tiers correspondent à un *Cloud* privé. Ces informations ne sont pas directement disponibles pour les banques mais par recoupement les ordres de grandeur semblent similaires.

ce processus, le Responsable de la Sécurité des Systèmes d'Information (RSSI) et les services informatiques conseillent les métiers et examinent les conditions d'intégration de la prestation au sein du système d'information. Un grand groupe bancaire indique qu'en cas d'évolution importante, le comité stratégique serait sollicité. Un groupe mutualiste précise que la décision d'engagement dans une prestation de *Cloud computing* ne pourrait provenir que de sa DSI. Une petite banque indique que cette décision serait prise par son directeur général en concertation avec le RSSI.

3. Mesures d'accompagnement requises

La **nécessité d'un environnement juridique davantage sécurisé** est clairement un point d'accord, les offres actuelles de *Cloud computing* semblant offrir peu de garantie sur le respect des dispositions relatives à la protection des données personnelles. Aussi, certaines clauses contractuelles comme celles permettant de restreindre la sous-traitance en dehors de l'Union européenne, une clause d'audit, une clause exigeant le stockage des données dans l'Union européenne semblent nécessaires. Pour d'autres entreprises, il conviendrait d'obtenir des engagements plus forts du prestataire sur la protection et la confidentialité des données personnelles, leur localisation et la réversibilité de la prestation. Un grand groupe bancaire et une compagnie d'assurance pencheraient pour une protection de type « *Safe harbor*[4] »à moins qu'une offre européenne ne se développe. Deux grandes entreprises du secteur de l'assurance privilégieraient une implantation européenne des données. Un autre groupe bancaire international aurait une préférence pour des fournisseurs français ou européens. A contrario, certaines entreprises du secteur de l'assurance considèrent que l'environnement juridique « classique » appliqué aujourd'hui à l'infogérance est suffisant, le *Cloud Computing* n'étant qu'une forme particulière d'externalisation informatique.

Parmi les mesures techniques de sécurité, le **chiffrement systématique des données** est la mesure qui revient le plus souvent, notamment pour protéger les données dont la localisation n'est pas connue. Un grand groupe bancaire précise toutefois que si le chiffrement des données lors du transport est obligatoire, il est plus complexe à mettre en œuvre pour le stockage. De grands groupes internationaux souhaitent que le chiffrement soit mis en œuvre par le déploiement d'une infrastructure à clés publiques qui ne serait pas gérée dans le *cloud*. Un grand groupe international (secteur assurance et banque) considère que le chiffrement n'est utile que pour les données sensibles (sans toutefois en donner de définition) et que l'anonymisation peut être utilisée dans les environnements hors production. Des assureurs souhaitent que les habilitations soient gérées par le donneur d'ordre et exigent le cloisonnement des données entre les différents clients du fournisseur.

Concernant les mesures techniques permettant d'éviter la perte de données, la réponse majoritaire est la mise en place d'un **plan de continuité d'activité avec une réplication des données sur des sites distincts**. Un grand groupe bancaire rappelle l'importance d'un secours hors région. Un autre groupe bancaire veut tester régulièrement les fonctions de sauvegarde et s'assurer que la copie est distante du site primaire. Cet établissement recommande de disposer d'un plan de secours testé par un organisme indépendant.

La **nécessité d'auditer régulièrement le prestataire et le service** est mise en avant dans la quasi-totalité des réponses. Un grand groupe international considère même que l'audit est un préalable à la souscription du service avec le prestataire. Un grand nombre d'entreprises rappellent les bonnes pratiques constituées par l'obtention des résultats d'audit des prestataires, la réalisation d'audits par l'entreprise, la réalisation de tests d'intrusion et de vulnérabilité (même si certains signalent toutefois que cela n'est pas toujours possible sur un *cloud* public). Les entreprises attendent une transparence de la part du fournisseur sur ses résultats d'audits internes mais aussi sur ses exercices de secours et ses incidents. Certains pensent que la certification du prestataire et l'accès à ses rapports de certification peuvent répondre aux besoins de contrôle. Une entreprise attend la mise en place de labels ou de certifications qui garantiraient que la prestation se déroule sur une zone géographique identifiée.

Beaucoup insistent sur la **nécessité pour le prestataire de s'engager** sur la continuité du service (durée d'indisponibilité maximale acceptée et perte de données maximale admissible), sur la localisation et la traçabilité du stockage des données, sur le cloisonnement des

[4] L'UE interdit que les données personnelles de ses citoyens sortent de son territoire. Mais les États-Unis ont obtenu que les données puissent sortir à condition d'offrir un environnement de protection équivalent et le département du Commerce a mis en place un dispositif de certification des entreprises américaines qui voudraient héberger des données personnelles européennes. Ce dispositif, connu sous le nom de « *Safe Harbor* », permet aux entreprises américaines telles Google, Microsoft ou Amazon de travailler en Europe sans y avoir de centres informatiques. Toutefois il ne crée pas d'exception au *Patriot Act* ni à la loi FISAA : les prestataires américains, même s'ils respectent le « *Safe Harbor* », sont tenus de remettre aux agences gouvernementales les données qu'elles demanderaient dans les conditions prévues par ces lois.

données en particulier pour un *cloud* public. Les entreprises précisent que tous ces éléments liés à la prestation de *Cloud computing* doit faire l'objet d'un *Service Level Agreement*. Un grand bancassureur international considère que le renforcement des obligations du prestataire doit se faire sur la base d'une analyse de risque préalable. Un autre groupe international (secteur banque et assurance) propose que le prestataire informe six mois à l'avance son client d'un changement de localisation des données et impose au prestataire une information en cas d'incident.

La nécessité d'obtenir une garantie du prestataire sur la réversibilité de la prestation (en particulier pour un SaaS) est rappelée, considérant qu'une clause contractuelle, parfois dénommée plan de réversibilité, doit être incluse. Ce plan doit décrire le format des données restituées, définir les conditions de restitution de ces données, traiter la question de leur propriété et de leur destruction et définir le délai de restitution. Un grand groupe international précise que pour s'assurer de la réversibilité, il faudrait disposer des moyens de récupération massive des données, tester régulièrement les outils et maintenir des compétences en interne. La réversibilité peut prendre la forme d'un transfert de données à un nouveau prestataire de *Cloud computing* sans obligatoirement passer par la ré-internalisation ; un groupe d'assurance considère que la portabilité vers un autre fournisseur est le plus simple à gérer.

4. Adéquation de l'environnement réglementaire

Les avis sont partagés sur l'adéquation de l'environnement réglementaire tant du coté bancaire que du côté de l'assurance.

Du côté bancaire, pour plusieurs établissements, les obligations de contrôle des prestataires –droit d'audit notamment– résultant du règlement CRBF n° 97-02 sont difficiles à tenir, particulièrement dans le cas des *Clouds* publics. Un grand groupe international indique qu'il faudrait exiger de la part du prestataire la conformité aux règles nationales assurant la protection des données personnelles pour chacun des pays dans lesquels il a des ressources informatiques. Deux grands groupes considèrent d'ailleurs que l'évolution de la réglementation dépasse le cadre français et même européen, puisqu'un fournisseur de *Cloud computing* peut exercer son activité depuis n'importe quel pays dans le monde ; dans ce cadre, plusieurs sociétés penchent pour un accroissement de la responsabilité du prestataire (notion de coresponsabilité du traitement) comme le prévoit le projet de révision de la directive 95/46/CE sur la protection des données[5]. Enfin, un grand groupe international juge que le *Cloud computing* n'est compatible avec la réglementation que si les offres sont bridées avec des exigences de localisation, de résilience et de contrôle mais, ces contraintes lui feraient perdre de son intérêt.

Du côté assurance, un organisme estime que les dispositions de l'article R 336-1 du Code des assurances, à titre d'exemple, ne contredisent pas l'utilisation raisonnée du *Cloud computing*. Toutefois, la plupart des organismes considèrent qu'avant de permettre une gestion des données à caractère personnel, les offres de *Cloud computing* devront se conformer aux dispositions figurant dans la loi Informatique et Libertés, une précision des responsabilités devant être apportée notamment pour les cas de sous-traitance démultipliée. Certains assureurs souscrivent également à l'idée d'un accroissement de la responsabilité du prestataire dans la gestion du traitement. Un groupe souhaiterait que les autorités mettent en place un processus de labellisation des sous-traitants offrant des services de *Cloud computing*. Enfin, un assureur considère que le cadre réglementaire est très strict pour les activités soumises à agrément (données de santé) et doit régulièrement évoluer avec les technologies.

5. Principaux enseignements et bonnes pratiques pouvant être dégagés.

Au vu des enseignements tirés de ces premières analyses, certaines bonnes pratiques paraissent se dégager en matière de recours à des prestations de *Cloud computing* dans les secteurs de la banque et de l'assurance.

Tout d'abord, une définition multicritères, inspirée de celle donnée par le *National Institute of Standards and Technology,* et qui tient compte de la nature évolutive de ces services (apparition de nouveaux prestataires, de nouvelles offres, …) peut être retenue. Cette définition multicritères présente l'avantage de bien distinguer les types de services et leurs risques associés.

L'ACP porte une attention particulière aux prestations susceptibles d'être mises en œuvre par les sociétés des secteurs de la banque et de l'assurance et qui reposeraient en tout ou partie sur des solutions de *clouds* publics ou hybrides, c'est-à-dire des solutions proposées par une

[5] A contrario, le règlement CRBF n° 97-02 est suffisamment large et bien adapté pour un établissement. Un autre groupe bancaire ajoute même que l'environnement réglementaire est adapté et convient déjà à l'infogérance.

entreprise spécialisée à destination d'un grand nombre de clients, ou dans lesquelles la localisation des données est inconnue, ou lorsque la prestation est accessible depuis le réseau Internet. Dans les points qui suivent, c'est à ces différents cas qu'il est fait référence par l'expression *Cloud computing*.

Les prestations de type *Cloud computing* se distinguent de l'externalisation classique des prestations informatiques de type infogérance. Le *Cloud computing* transforme les fonctions Systèmes d'Information (SI) de manière permanente, qu'il s'agisse des caractéristiques des services délivrés (alignement sur celles du *Cloud* principalement dans un objectif d'amélioration de la qualité du service rendu) ou de l'origine de ces services (externalisation, en premier lieu afin de réduire les coûts d'investissement).

La maturité grandissante des offres du marché est susceptible de conduire de nombreuses entreprises à vouloir recourir au *Cloud computing*. Il apparait ensuite nécessaire d'anticiper les changements à venir à travers l'intégration du *Cloud computing* dans les stratégies d'évolution des systèmes d'information des entreprises qui devra en particulier couvrir la définition d'une politique d'entreprise claire relative à la nature des données et des traitements qu'il est acceptable d'externaliser.

Les risques liés au *Cloud computing* étant nombreux et nouveaux (sans qu'un recul suffisant soit disponible), l'utilisation de services *cloud* ne devrait toujours résulter que de la démonstration que les avantages qu'ils apportent valent les risques pris. La question centrale de toute réflexion sur l'utilisation du *Cloud computing* est la maîtrise des informations et leur degré de sensibilité.

En termes d'organisation, le *Cloud computing* est un vecteur de transformation majeur des processus opérationnels, de l'allocation des rôles et responsabilités, et donc de l'organisation des fonctions SI elles-mêmes mais aussi des relations entre la fonction SI, le RSSI les différents métiers. L'introduction du *Cloud computing* va également avoir un impact majeur sur les profils nécessaires au sein des fonctions SI et pose donc un problème de gestion des compétences.

Au-delà des questions d'organisation et de compétences que soulève le recours au *Cloud computing*, les risques spécifiques qui s'ajoutent aux risques classiques engendrés par toute externalisation informatique doivent être parfaitement maîtrisés dans les domaines de la banque et de l'assurance. Les singularités du *Cloud computing* visent notamment les critères de sécurité de l'information :

- **Confidentialité des données :** la protection des données sensibles et personnelles, de même que le respect du secret bancaire, sont particulièrement difficiles au sein d'infrastructures mutualisées et potentiellement accessibles aux régulateurs locaux. Le manque de visibilité sur la localisation des données et donc sur la réglementation applicable ainsi que le nombre de parties prenantes dans une solution de *Cloud computing* accentuent ce risque. La question de la confidentialité des données se pose également en termes d'assurance de leur destruction effective en cas d'arrêt de la prestation, y compris sur les sauvegardes dans des sites qui peuvent être dispersés ;

- **Disponibilité des données et des traitements :** la dispersion des données ainsi que la multiplicité des intervenants fragilisent l'entreprise dans sa capacité à s'assurer de ces critères. La relation asymétrique qui lie le fournisseur à son client, caractérisée notamment par la difficulté d'inclure des engagements contraignants (clauses de pénalité) sur un niveau minimum de disponibilité, peut renforcer ce risque ;

- **Intégrité des données :** le recours à un prestataire de C*loud computing* crée un risque d'atteinte à l'intégrité globale du système d'information en raison de la perte d'expertise technique, voire de dépendance au fournisseur. Plus spécifiquement, le pilotage par l'organisme client des prestations de type *Cloud computing* est plus distant et restreint que dans les autres cas d'infogérance, induisant dans la durée un risque important de dépendance : perte de la connaissance du système d'information et des compétences attenantes et asservissement aux technologies spécifiques du fournisseur, pouvant empêcher la réversibilité de la prestation ;

- **Contrôle et preuve :** le déploiement d'un dispositif de contrôle interne adapté est rendu complexe par les difficultés à mettre en place une relation contractuelle équilibrée, à auditer le prestataire (multiplicité des intervenants, localisation géographique potentiellement mondiale, …) et à identifier la réglementation applicable aux données.

- **Urbanisme et organisation :** le recours à une prestation informatique de type cloud est susceptible de provoquer des problèmes d'intégration dans le système d'information et d'en diminuer à moyen terme sa flexibilité et sa capacité d'évolution. Les difficultés induites sont à la fois techniques (intégration potentiellement inadéquate d'un composant très standardisé

dans un système d'information) et parfois organisationnelles (capacité de l'organisation informatique à s'adapter à des évolutions du service *Cloud* parfois très fréquentes).

Tout en reconnaissant l'intérêt qui peut être trouvé à recourir à des prestations de *Cloud computing*, il est important de ne pas s'engager dans une telle solution sans avoir identifié les risques associés afin d'en assurer une parfaite maîtrise. A ce titre, la conformité à la réglementation existante en matière de contrôle interne (R. 336-1f du Code des Assurances, R. 211-28f du Code de la Mutualité et R. 931-43f du Code de la Sécurité Sociale ou règlement CRBF n°97-02) est un élément incontournable :

- en matière d'externalisation de prestations essentielles ou d'autres tâches importantes, il n'est pas évident que des fonctions considérées comme « support » ne soient pas en pratique à considérer comme essentielles ou importantes, eu égard à la place qu'elles prennent dans la réalisation de certains services et pour la continuité de l'activité (ressources informatiques notamment) ;

- sur la protection de la sécurité et de la confidentialité des données, les dispositions de la règlementation trouvent à s'appliquer également aux services *Cloud*. Les services actuellement mis dans le *Cloud* peuvent contenir des données de la clientèle, donc des informations confidentielles, voire sensibles, et couvertes par le secret professionnel (gestion de la relation client, messagerie, archivage…). L'application de la réglementation doit donc se faire pas simplement au vu du caractère « fonction support » ou « fonction métier » au sein de l'entreprise, mais au regard de la nature des données susceptibles d'être placées dans ces environnements.

L'utilisation des services *Cloud* tend désormais à se développer, sous l'impulsion des métiers qui apprécient la facilité d'usage et la rapidité de mise en œuvre et l'engagement dans ce type de prestation se fonde parfois uniquement sur une décision du métier utilisateur, après consultation du Responsable de la Sécurité des Systèmes d'Information. Au contraire, vu l'importance des risques, l'engagement dans ce type de prestation devrait systématiquement impliquer les instances dirigeantes de l'établissement, au titre de la bonne gouvernance du système d'information. Ces instances devraient se prononcer en disposant du point de vue indépendant du responsable de la filière risques et du RSSI s'il n'appartient pas à cette filière.

Lorsqu'elles concernent des activités essentielles (et/ou confidentielles), la mise en œuvre des prestations *Cloud* doit s'accompagner de mesures de maîtrise du risque adaptées :

- **Juridique** : l'encadrement contractuel de la prestation est impératif. Les mesures de protection des données mises en œuvre par le prestataire doivent être évaluées avant souscription du service. Concernant la protection des données personnelles, la prestation doit se conformer à la Directive européenne 95/46/CE et plus largement aux règles de protection de la propriété intellectuelle. Certains éléments transférés dans le *Cloud* sont susceptibles d'entrer dans le capital de la propriété intellectuelle de l'entreprise et doivent faire l'objet d'une clause contractuelle. Par ailleurs, tout changement dans la nature de la prestation doit être maîtrisé, y compris dans les versions logicielles. L'entreprise cliente d'une offre *Cloud* doit mettre en place un pilotage contractuel continu, en s'appuyant sur des clauses de pénalité à actionner lors d'insuffisances dans le service rendu par le prestataire. Enfin, l'encadrement contractuel doit également permettre d'obtenir la visibilité sur l'organisation du prestataire, notamment en termes de sous-traitance éventuelle ;

- **Technique** : en l'absence d'anonymisation, les données confidentielles confiées au prestataire doivent être chiffrées lors du transport ainsi que pendant le stockage. La solution de chiffrement doit être maîtrisée par le propriétaire des données (ce qui implique que la gestion des clés soit opérée par l'entreprise soumise au contrôle de l'ACP) et une attention particulière doit être portée à la ségrégation des environnements entre les entreprises clientes et à la gestion des habilitations ;

- **Contrôle du prestataire** : la capacité d'audit et le droit de le faire pour l'ACP est une clause contractuelle essentielle à toute prestation de *Cloud computing*. La réalisation régulière d'audit est attendue. La réalisation de tests d'intrusion et de vulnérabilité est nécessaire au contrôle de la prestation ainsi que l'accès à des traces d'audit préalablement identifiées (le principe de cloisonnement des données entre différents clients s'applique également à ces traces). La seule certification du prestataire ne doit pas être considérée comme une mesure de maîtrise des risques suffisante. Il est nécessaire de tenir à jour en permanence la liste des fournisseurs de *Cloud computing* ainsi que la liste des prestations qui leur sont confiées ;

- **Continuité de la prestation** : l'existence des conventions de service (en anglais SLA « service level agreement ») est essentielle ; elles permettent de formaliser les attentes de l'entreprise cliente. Des engagements précis du

prestataire sont attendus en matière de continuité d'activité (notamment la durée maximale d'interruption et la perte de données maximale admissibles). Le suivi de la prestation doit s'appuyer sur des *reportings* portant sur la disponibilité, les incidents de sécurité et la localisation des données ;

- **Réversibilité de la prestation** : les conditions de réversibilité doivent être définies lors de la souscription du service. Les questions du format des données restituées et de leur destruction doivent être couvertes dans le contrat liant les parties. Cette capacité à se désengager du prestataire entraîne également des contraintes du côté de l'organisme client. Celui-ci doit en effet s'assurer de sa capacité à reprendre l'activité externalisée ou à la transmettre à un autre prestataire avec une réactivité suffisante (gestion de la connaissance fonctionnelle, applicative et technique, capacité à positionner des ressources et à les faire monter en compétence, budget à engager, etc.). La dépendance au fournisseur de la solution de *Cloud computing* doit être évaluée régulièrement ;

- **Intégration et urbanisme du système d'information** : la mise en place d'une organisation de la fonction informatique adaptée, prenant en compte toutes les contraintes extérieures à l'entreprise induites par un service Cloud, ainsi qu'une maîtrise de l'urbanisme du système d'information et de son évolution, sont des pré-requis pour le recours à un service de *Cloud computing*. Il est important que la fourniture de services informatiques reste sous la responsabilité de la fonction SI afin que celle-ci soit à même de piloter effectivement la cohérence d'un système d'information élargi.

L'ensemble de ces bonnes pratiques s'inscrivent dans le cadre plus large défini pour le contrôle des prestations essentielles externalisées, y compris l'infogérance classique. Les attentes en termes de gouvernance des décisions, d'analyse des risques, de contractualisation, de pilotage et de contrôle interne des prestations de *Cloud computing* sont donc similaires à celles qui prévalent aujourd'hui dans le contrôle prudentiel.

Annexe : Enquête relative au *Cloud Computing* (questionnaire envoyé)

Objectif de l'enquête

En consultant sur le thème du « Cloud Computing », l'ACP souhaite :

- mesurer si ce concept, cette offre technologique et commerciale, fait apparaître de nouveaux risques dans les secteurs de la banque et de l'assurance,
- apprécier si les politiques de sécurité et les textes réglementaires existant les couvrent suffisamment,
- recueillir des suggestions.

1. Caractéristiques du cloud computing

Le « cloud computing » consiste à déporter sur des serveurs distants des données et des traitements informatiques traditionnellement localisés sur des serveurs locaux, voire sur le poste de l'utilisateur. Il permet l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées généralement facturées à l'usage.

Le « cloud computing » fournit dans ses déclinaisons les plus courantes des ressources de type :

- Infrastructure informatique, comme de la puissance de calcul, des machines virtuelles incluant un système d'exploitation, du stockage, des services de sauvegarde…On parle alors d'« Infrastructure as a Service » (IaaS) ;
- Plateforme de développement et d'exécution intégrée, reposant sur un catalogue de composants logiciels et techniques standardisés dont l'infrastructure sous-jacente est masquée à l'utilisateur. Il s'agit alors de « Platform as a Service » (PaaS) ;
- Solution applicative répondant à un domaine d'utilisation précis supportant une fonction métier (CRM, gestion financière…) ou un service transverse (messagerie, outils collaboratifs…) dans le cadre d'une offre de « Software as a Service » (SaaS).

Il existe plusieurs formes de « cloud computing » :

- les clouds privés internes, gérés en interne par une entreprise pour ses besoins sur des infrastructures lui appartenant,
- les clouds privés externes, dédiés aux besoins propres d'une seule entreprise ou d'un groupe d'entreprise, mais hébergés chez un prestataire,
- les clouds publics[6], gérés par des entreprises spécialisées qui louent leurs services à de nombreuses entreprises,
- les clouds hybrides qui combinent de manière dynamique les clouds publics et privés.

Le cloud public est une forme particulière de gérance de l'informatique, pour laquelle la prestation est mutualisée pour un grand nombre de clients, et l'emplacement des données dans le nuage n'est généralement pas porté à la connaissance des clients.

La définition du « cloud computing » donnée par le Gartner est :

« *Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies* »

Dans la suite de l'enquête, les questions portent sur les formes de « cloud computing » faisant intervenir un prestataire (clouds privés externes, clouds publics et clouds hybrides).

*

Question 1.1 – Ces éléments de définition vous paraissent-ils pertinents pour caractériser les services de « cloud computing » dans les secteurs de la banque et de l'assurance ? Voyez-vous d'autres caractéristiques permettant de préciser le concept ?

Question 1.2 – Dans les secteurs de la banque et de l'assurance, quels sont les principaux éléments différentiateurs entre le « cloud computing » et une infogérance classique ?

Question 1.3 – Compte tenu de vos infrastructures existantes, le « cloud computing » peut-il répondre à un enjeu économique ?

Question 1.4 – L'état actuel des offres commerciales de type « cloud computing » vous paraît-il présenter des risques ? (préciser)

[6] Le mot « public » renvoie ici à l'acception généralement utilisée par les acteurs du cloud computing, c'est-à-dire un environnement ouvert et multi-client. Il ne fait donc pas référence à des initiatives de la sphère étatique.

2. Les cas d'usage du « cloud computing »

Question 2.1 – Quels sont pour vous les avantages incitant à aller vers une démarche de « cloud computing » dans vos domaines d'activité ? Par quelle(s) direction(s) cette démarche est-elle initiée ?

Question 2.2 – Quels sont pour vous les facteurs limitant l'adoption du « cloud computing » dans vos domaines d'activité ?

Question 2.3 – Quels sont les applications ou services informatiques pour lesquels vous recourez ou vous pourriez recourir à des services de « cloud computing » :

- **Dans le domaine des fonctions supports (RH, Comptabilité, Stockage des données, archivage des données,…) ?**
- **Dans le domaine de la bureautique et des outils collaboratifs (messagerie, site d'équipe, ...) ?**
- **Dans le domaine de la banque de détail ?**
- **Dans le domaine de la banque de financement et d'investissement ?**
- **Dans les domaines spécialisés, tels que le crédit aux particuliers ou aux entreprises ?**
- **Dans le domaine de l'assurance Vie ?**
- **Dans le domaine de l'assurance IARD ?**
- **Dans le domaine de Réassurance ?**
- **Dans le domaine spécialisé de la Santé ?**
- **Autres…**

Et pour quel type de « cloud computing » ?

Question 2.4 – A contrario, quels sont pour vous les applications ou services informatiques pour lesquels vous ne souhaitez pas recourir à un prestataire de services cloud (expliquer) ?

Question 2.5 – A quel niveau de la gouvernance de votre entreprise ce type de décision est (serait) pris ?

Question 2.6 – Votre établissement offre-t-il lui-même des services de « cloud computing », par exemple à ses clients ou à d'autres établissements ?

3. L'environnement juridique du « cloud computing »

Question 3.1 – Quel est l'état de vos réflexions concernant les contraintes juridiques pesant sur le stockage, potentiellement extraterritorial, et la protection des données ?

Question 3.2 – Si vous avez déjà souscrit à une offre de « cloud computing », quelles ont été vos exigences contractuelles vis-à-vis du fournisseur du service de cloud en termes de sécurité des données et des traitements (confidentialité, intégrité, disponibilité) et d'auditabilité des services fournis ?

Question 3.3 – Dans l'hypothèse contraire, quelles seraient vos principales exigences contractuelles relatives à la protection des données et la maîtrise de la prestation ?

Question 3.4 – Comment considérez-vous les différents types de « cloud computing » au regard des obligations relatives aux prestations essentielles externalisées ?

Question 3.5 – L'environnement réglementaire encadrant la sous-traitance des activités soumises à agrément vous paraît-il adapté aux caractéristiques des services de « cloud computing » ?

Question 3.6 – L'environnement légal et réglementaire (européen et national) relatif à la protection des données vous paraît-il adapté aux caractéristiques des services de « cloud computing » ?

Question 3.7 – En cas d'insatisfaction des services rendus, quels sont pour vous les éléments déterminants pouvant garantir le succès d'une ré-internalisation (réversibilité, …) ?

4. Les risques et les mesures de sécurité associés au cloud computing

La sécurité des données est un enjeu primordial pour les entreprises. Avec le « cloud computing », la gestion de la sécurité se trouve fortement déléguée au prestataire pour couvrir les risques portant sur :

- la confidentialité et l'intégrité des données (y compris lors de l'arrêt de la prestation),
- la perte de données,
- la continuité de service,
- la qualité de service.

Question 4.1 – Quelle méthodologie d'analyse de risque utilisez-vous ou utiliseriez-vous pour identifier les objectifs de sécurité à atteindre et définir les exigences de sécurité ?

Question 4.2 – Le besoin de protéger les actifs (données et applications ou services d'infrastructure) nécessite des mesures de sécurité adaptées, lesquelles vous paraissent incontournables pour :

- Assurer la confidentialité des données ?
- Éviter la perte de données ?
- Assurer la continuité et la qualité de service ?

Question 4.3 – Selon vous, la non maîtrise de la localisation des données doit-elle induire des mesures de sécurité particulières ? Le chiffrement des données avant qu'elles ne soient hébergées dans le cloud est-il une nécessité et vous paraît-il applicable ? Si oui, pour quels éléments considérez-vous qu'il doive être mise en œuvre (transport des données, stockage des données, modalités de gestion des clés, etc.) ?

Question 4.4 – En cas d'usage de « cloud computing », comment contrôlez-vous ou contrôleriez-vous le niveau de sécurité ? La possibilité de réaliser un audit est-elle une condition sine qua non à l'utilisation d'un service de « cloud computing » ?

61, rue Taitbout
75009 Paris
Téléphone : 01 49 95 40 00
Télécopie : 01 49 95 40 48
Site internet : www.acp.banque-france.fr