Le centre d'excellence
et de partage du Sourcing

Monter un projet Cloud : Les questions incontournables à se poser pour les directions métiers

Synthèse du travail de la Commission Juridique - EOA France sur le Cloud Computing
Novembre 2013

Introduction

Nouvelle forme de sourcing et de fourniture de services rendue possible par une puissante évolution technologique, le Cloud Computing consiste à mettre à disposition via les réseaux, à la demande, un ensemble de moyens et/ou services, moyennant un mode de facturation basé sur l'utilisation qui en est faite. Le Cloud a piqué la curiosité de la commission juridique de l'EOA France, qui s'est intéressée à l'une de ses conséquences immédiates les plus saillantes, à savoir l'émancipation des directions métiers (ou Business Units) vis à vis tant de la DSI que de la direction juridique, dans le montage de leurs projets.

Dans un projet de sourcing traditionnel, nombreuses sont les directions impliquées : la Direction des Systèmes d'Information joue souvent un rôle prépondérant car c'est elle qui pilote la rédaction du cahier des charges, aide l'utilisateur à recenser ses besoins, choisit les prestataires, définit les règles de sécurité et techniques, etc. C'est elle encore qui arbitre, assure et garantit la cohérence, contribue aux processus opérationnels et contrôle le prestataire. De son côté, la direction juridique est impliquée sur le montage du projet, les consultations à mener et le volet contractuel. En outre, lorsque des problématiques sociales se posent, rien ne peut se faire sans l'implication de la DRH. Enfin, peu de projets échappent au contrôle de la direction des achats, souvent en première ligne dans le montage de ces opérations et le choix des prestataires.

Il s'ensuit toutes sortes de points de contrôle internes, dont la validation garantit le succès de l'opération. Il s'ensuit également une certaine lourdeur et un coût.

Dans un projet Cloud, cette organisation de la prise de décision n'existe plus : les directions métiers concernées sont désormais à même de monter toutes seules leurs projets et, de fait, peuvent s'émanciper des directions précitées, autrefois incontournables. Ce sont d'ailleurs elles, désormais, qui souvent détiennent les budgets nécessaires pour mettre en œuvre ces projets.

Ce faisant, elles prennent le risque de s'émanciper également des nécessaires contrôles internes, créant - souvent par ignorance - sans toujours en avoir pleinement conscience, toutes sortes de nouveaux risques pour l'entreprise et un nouveau cloisonnement au sein de celle-ci, paradoxalement antinomique avec la promesse initiale du Cloud qui prétend à la globalité et au décloisonnement. De l'impossibilité de récupérer ses propres données - du fait de problèmes techniques non anticipés - à la perte pure et simple de celles-ci - car imprudemment confiées à un prestataire non-pérenne - ces risques sont bien réels, comme l'ont démontré certaines affaires récentes.

C'est vraisemblablement à la « simplicité » présumée du Cloud que l'on doit cette évolution. Le Cloud est en effet devenu synonyme de simplicité, de souplesse, d'efficacité et de gains de productivité (souvent, avouons-le, grâce à la multiplication impressionnante des offres commerciales vantant ces caractéristiques, un peu à la manière de la méthode Coué…).

Or, cette simplicité présumée ne va pas de soi, et à bien y regarder, il est peu de projets Cloud aujourd'hui qui peuvent faire l'économie d'une plus grande responsabilisation de la part de ceux qui les montent.

Il convenait donc d'informer les directions métiers qui s'engagent dans cette voie en dressant un inventaire des diverses étapes qu'elles devraient suivre sur les plans stratégiques, techniques, opérationnels et juridiques, pour que leur choix d'une solution Cloud se traduise par une valeur ajoutée effective et significative pour leur entreprise, et non par une prise de risque non maîtrisée.

C'est l'objet de cette nouvelle publication de l'EOA France, qui entend fournir un outil pragmatique d'assistance au montage d'un projet Cloud, en recensant les différentes questions à se poser lors de la mise en œuvre de ce type de projet, tout en les replaçant dans leur contexte.

Ce travail n'a toutefois pas pour objectif d'être exhaustif ; les auteurs ont surtout souhaité donner des pistes pour aider les directions Métiers à mieux cerner leurs nouvelles responsabilités. En les amenant à se poser, de façon approfondie et circonstanciée, la question « *suis-je bien éligible au Cloud* » ?, ce billet entend les aider à piloter sereinement un projet Cloud et à délivrer toute la valeur business attendue de celui-ci pour l'entreprise.

Brève définition du Cloud

Le Cloud c'est essentiellement un pas vers une économie de « SERVICES ». L'entreprise utilisatrice cesse d'investir dans des moyens de production qui lui sont propres (équipement, logiciels), pour se tourner vers le monde du service, dans lequel toutes les solutions antérieurement mises en œuvre en interne, à grand renfort de projets et d'investissements, sont désormais disponibles en tant que services, moyennant un coût fonction de l'utilisation effective. Le Cloud recouvre classiquement trois modèles de services :

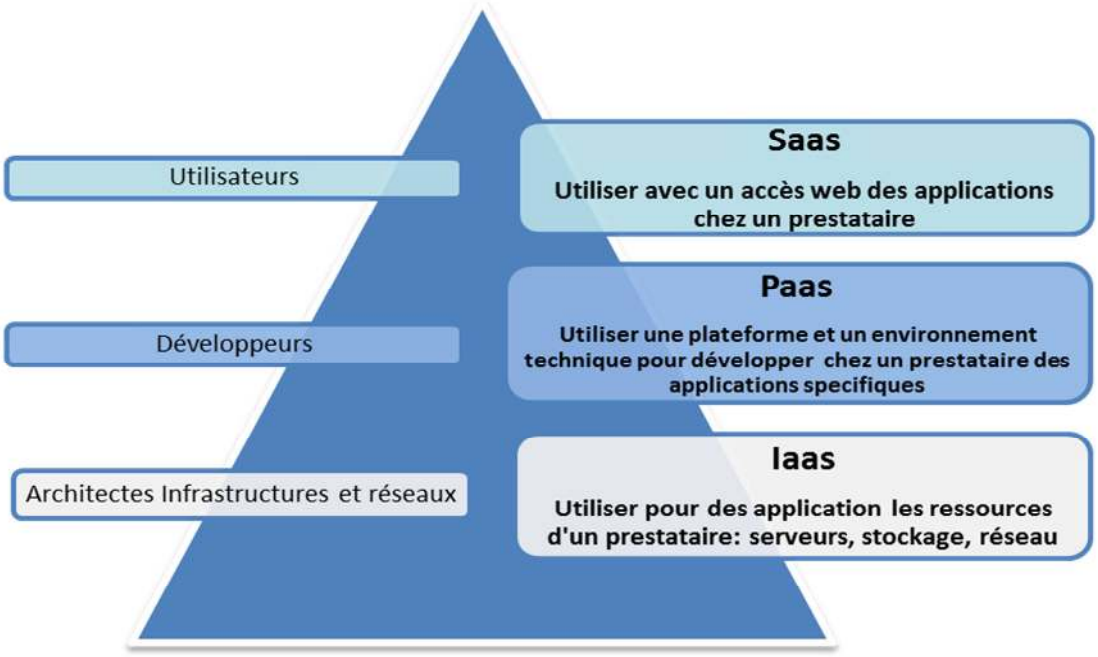
- **L'IaaS** (Infrastructure as a Service) se présente comme la mise à disposition de capacités de traitements (serveurs, stockages), de services réseaux et logiciels avec des environnements de machines virtuelles, le prestataire assurant la mise en œuvre, la gestion et la maintenance de ces environnements. *Exemple :* Stockage, machine virtuelle Amazon (EC2).

- **Le PaaS** (Platform as a Service) intègre la même plate-forme que l'IaaS mais propose une couche supplémentaire sur laquelle le client développera des services et des applications sans avoir à gérer et à contrôler l'infrastructure Cloud. Il contrôle les applications déployées et peut configurer l'environnement technique applicatif correspondant. Le prestataire assure la responsabilité de l'exploitation, du déploiement et de la maintenance de la plate-forme technique en condition opérationnelle.

- **Le SaaS** (Software as a Service) permet au client d'accéder à ses applications via le réseau par un simple navigateur web. Le prestataire déploie, gère et maintient toute l'infrastructure technique et logicielle Cloud, permettant ainsi à son client de s'affranchir totalement de toute cette dimension (*Exemple :* Microsoft 365°, Google Apps, Salesforce).

D'autres distinctions sont également possibles, selon que l'on est en présence d'un cloud public (totalement externalisé et reposant sur des infrastructures mutualisées), privé (interne ou externalisé) ou hybride (mélange des deux). Chaque solution a ses particularités qu'il convient de bien appréhender.

Ce billet envisage pour sa part exclusivement le cas du projet visant des services de Cloud public, car c'est celui qui est le plus novateur et qui présente les problématiques les plus sérieuses.



Dans les trois cas, même si la voie choisie - celle de l'acquisition d'un service - apparaît simple et peu engageante, la mise en œuvre d'un projet Cloud induit des choix techniques et juridiques essentiels, notamment en matière de sécurité, de confidentialité, de localisation et d'intégration des données, qu'il convient donc de recenser et d'adresser en temps utile, sauf à prendre le risque de passer totalement à côté.

Les questions incontournables que les métiers doivent se poser

Nous avons choisi de recenser ces problématiques sous forme de questions, car si celles-ci pointent bien vers des problématiques communes à toutes les entreprises, il n'existe pas nécessairement de réponses valables pour toutes. Nous avons aussi choisi de les exprimer de façon très directe, en adoptant la perspective de l'utilisateur, afin de lui permettre de s'impliquer plus facilement dans la problématique et de se projeter ainsi dans son projet.

Ces questions sont regroupées en plusieurs thèmes :

A. Alignement de ma stratégie avec celle de mon prestataire

B. Définition du besoin, du service et du prix

C. Intégration du Cloud dans le SI de mon entreprise

D. Protection et sécurité des données dans le Cloud

E. Licences et droits de propriété intellectuelle

F. Entrée et sortie du Cloud : Migration – Réversibilité

A. MA STRATÉGIE EST-ELLE ALIGNÉE AVEC CELLE DE MON PRESTATAIRE ?

En souscrivant à un service Cloud, le client utilisateur va se trouver profondément lié à la stratégie du prestataire - en d'autres termes, on achète la stratégie du prestataire. Il convient donc de s'interroger sur la compatibilité entre sa propre stratégie et celle du prestataire, et leurs évolutions futures.

Il convient à cet égard de prendre en compte la durée prévisible de la relation.

La stratégie du prestataire

1. Quelle est la cible visée par le prestataire ? quelle est sa stratégie d'évolution produits / services ? De quelle visibilité puis-je disposer sur son évolution dans le temps ?

Il convient de s'assurer que les stratégies de l'un et de l'autre coïncident, dans la durée. Suis-je bien dans la cible du prestataire ? Pour combien de temps ? Si je n'y suis pas, je risque de me trouver rapidement en périphérie de ses préoccupations, avec pour corolaire un risque grandissant que le service me convienne de moins en moins.

Quel préavis mon prestataire est-il prêt à me donner au cas où il déciderait d'interrompre, ou de faire évoluer de manière très significative son service ? A la manière des dates de fin de support annoncé des éditeurs de logiciel, qui permettent d'anticiper la durée prévisible d'utilisation d'un logiciel, il est permis de demander des engagements précis sur ce point au prestataire de services Cloud.

➢ ***Pérennité***

2. Qu'est ce qui me permet de penser que le prestataire est pérenne ?

Quelle est son expérience dans les services proposés ? Quelle est sa structure financière ? Qui sont ses actionnaires ? Quelles sont ses perspectives financières ?
Le Cloud est devenu un « buzz word » qui est utilisé par toutes sortes d'intervenants pour son pouvoir d'attraction. Parce que ses enjeux sont essentiels pour le client utilisateur, je dois m'assurer que j'ai affaire à un intervenant sérieux et pérenne et que je ne ferai pas les frais d'une approche trop exclusivement commerciale du sujet.
Le parallèle à faire ici pour illustrer cette problématique est le cas Mégaupload, qui a vu des utilisateurs d'un service Cloud de type stockage, perdre la totalité de leurs données du jour au lendemain, sans espoir de jamais les recouvrer, en raison d'une interruption du service par les autorités.

➢ ***Pérennité***

3. Le prestataire est-il maître de son infrastructure ? Quels sont ses sous-traitants et quel est son écosystème ? Comment la maîtrise-t-il ?

Un prestataire qui maîtrise tous les éléments de son offre ne présente pas du tout le même profil de risque qu'un autre qui s'appuie sur des tiers pour des composantes essentielles de son offre (infrastructure notamment). Quel est le niveau de sous-traitance envisagé ? Une sous-traitance en chaîne est-elle possible ? Quelle connaissance (transparence) ai-je sur cette dimension et quels engagements mon prestataire est-il prêt à prendre ?

De fait, c'est toute la chaîne de sous-traitance qu'il convient de sécuriser, en s'assurant que par un réel « back-to-back », tous les engagements de mon prestataire pèsent également sur ses sous-traitants.

➢ ***Sécurité / Contrôle / Qualité***

4. Le prestataire est-il aligné avec ma politique de développement durable ?

Quelle est sa stratégie en la matière ? Puis-je disposer d'engagements précis ? Mesurables ?

➢ ***Conformité***

5. Quelle influence pourrai-je avoir sur la stratégie du prestataire ?

Que m'est-il proposé ? Une offre purement standard ou un partenariat, dans lequel je pourrai avoir une marge d'influence (seul ou avec d'autres) sur la stratégie de mon prestataire ? L'une comme l'autre peuvent me convenir, mais compter sur l'une alors que seule l'autre est réellement offerte peut créer de grosses déconvenues.

➢ ***Stratégie***

Ma stratégie

6. Ma stratégie de sourcing - à travers ce projet Cloud - est-elle alignée avec le reste de mon entreprise ? avec ses systèmes d'information ? avec sa stratégie financière (OPEX vs. CAPEX) ?

Le fait d'acheter un service plutôt que de le faire en interne est-il bien en phase avec la stratégie d'achat de mon entreprise - « make or buy » ou « make or rent » ? Quelles seront les conséquences de mon choix sur le reste de l'entreprise ? Par exemple, qu'adviendra-t-il des systèmes que j'utilise jusqu'à présent pour la finalité recherchée ? Quels coûts entraineront le « décommisionning » de ceux-ci, si c'est là la conséquence de ma décision d'évoluer vers le Cloud ?

➢ ***Coûts***

7. Quelle est ma stratégie en matière de données ?

Le choix du Cloud implique une dépossession, des flux de données et des risques externes. Suis-je aligné avec la politique de mon entreprise (Cloud privé / Cloud public) sur ce sujet ? Les risques de perte ou de divulgation des données transférées dans le Cloud - notamment s'il s'agit de données personnelles - ont-ils été bien anticipés et intégrés au niveau de mon entreprise dans son ensemble ?

➢ ***Sécurité / Conformité***

8. Un partenariat est-il possible/souhaité avec le prestataire ?

Quel est le poids de mon projet/mon entreprise pour le prestataire ? Un partenariat peut changer la donne pour la réussite d'un projet (beta tester, client pilote, partage d'expérience, enrichissement mutuel, etc.).

➢ ***Stratégie***

9. Suis-je prêt à prendre des engagements en contrepartie d'un investissement fait par le prestataire ?

De fait, le paiement à l'usage mis en avant dans les services Cloud déplace la responsabilité d'investir du client utilisateur vers le prestataire. Celui-ci demandera donc des contreparties sous forme d'engagements de la part du client (volumétrie et/ou durée des services souscrits) ou imposera des contraintes liées à la nature même de son modèle industriel. Jusqu'à quel point suis-je prêt à m'engager ? Ai-je bien mesuré la portée de l'engagement demandé ? Comment et dans quelles conditions puis-je sortir si je dois effectivement sortir ?

➢ ***Coûts / Stratégie***

B. QUELS SERVICES, POUR QUELS BESOINS, POUR QUEL PRIX ?

Les offres Cloud reposent, c'est leur modèle économique, sur un fort degré de standardisation. Il est donc critique de s'assurer que le service - par essence standardisé - que j'envisage de souscrire est bien compris et répond bien au besoin identifié.

Définition du besoin

10. Quel est mon besoin ? Où est-il exprimé ?

L'expression du besoin (ex : service d'hébergement, machine virtuelle, stockage, plate-forme, accès à des logiciels...) est fondamentale et sa formalisation écrite, complète, l'est tout autant. C'est de l'échec certain du projet qu'il s'agit si cette question est mal abordée.

Il faudra également dans ce cadre s'interroger sur les besoins périphériques, tels que la nécessité de prévoir des services d'intégration pour mettre en œuvre les services envisagés dans l'entreprise - volet critique et pourtant trop souvent négligé! (ex : comment s'assurer que mes applications existantes peuvent échanger des emails avec un service mail dans le Cloud ?).

Sauf à recréer de nouveaux cloisonnements dans l'entreprise, un service totalement indépendant du reste du SI n'aura que peu de valeur - il faudra donc l'interfacer, mais qui est en charge de recenser les interfaces nécessaires ? Qui devra les réaliser ? Les financer ?

➢ ***Coûts / Délais / Cloisonnement***

11. Comment ce besoin est-il actuellement rempli ? Par qui/quoi ? Quelles sont les autres directions impactées ?

C'est tout le volet transformation du projet qui sera potentiellement impacté par les réponses à ces questions : en d'autres termes, ma direction est-elle seule concernée (c'est rare…!) ou le projet risque-t-il d'impacter d'autres directions/fonctions de l'entreprise (c'est plus fréquent !).

Le projet présente-t-il un aspect social ? si oui, des consultations préalables des institutions représentatives du personnel seront requises, qui devront nécessairement impliquer la DRH. Un décommissionning des systèmes existants sera-t-il rendu nécessaire ? si oui, il aura des conséquences financières et potentiellement également sociales pour l'entreprise.

➢ ***Coûts / Responsabilité***

12. Pourquoi opter pour un service Cloud ?

Quel est mon objectif avec ce projet ? Celui-ci doit être clairement identifié et exprimé (ex : « je veux améliorer mon time-to-market »), afin d'être partagé avec le prestataire pressenti et les autres directions éventuellement impactées. En quoi cet objectif est-il atteint par la solution Cloud que j'envisage ?

➢ ***Stratégie / Coûts***

13. Ai-je pris en compte l'environnement réglementaire ?

Plusieurs contraintes réglementaires sont susceptibles de peser sur le projet (voir Focus Réglementaire ci-dessous). Suis-je bien au fait des contraintes réglementaires éventuellement applicables à mon activité ? aux traitements que j'envisage de porter dans le Cloud ? aux données qui vont y transiter ou y être transférées ? Si oui, sont-elles identifiées en tant que telles dans mon expression de besoins, de telle manière que mon prestataire en soit également bien informé ? Si non, qui peut m'aider à les identifier ?

Faire l'économie de cette analyse, c'est prendre le risque de se placer en infraction en n'étant pas informé de ses responsabilités.

➢ ***Conformité***

14. Puis-je m'appuyer sur le devoir de conseil d'un tiers (notamment le prestataire pressenti) quant à la bonne expression de mes besoins ou suis-je seul en cause ?

A défaut d'implication d'un professionnel (potentiellement le prestataire de services Cloud lui-même) pour m'assister sur ce volet, je n'aurai pas de recours si la solution n'est pas adaptée à mon entreprise/mes besoins et devrait assumer seul la responsabilité de l'échec.

De fait, beaucoup de fournisseurs d'offres Cloud rejettent actuellement cette responsabilité au motif du caractère standardisé de leur offre, affirmant que c'est à l'utilisateur du service qu'il revient exclusivement de prendre ses précautions sur ce point.

➢ ***Responsabilité***

Description du service

15. Où est décrit le service que j'achète ? Cette description est-elle suffisante et recouvre-t-elle pleinement le périmètre de mes besoins ?

Le diable est dans le détail! Le Cloud correspond à un service standardisé - la flexibilité réside dans le mode de tarification des services, pas dans leur consistance. A défaut de vérifier en temps opportun que la description du service correspond bien à ce que je crois acheter, le

réveil risque d'être douloureux. La consistance précise des services, leur durée, leurs limites doivent être précisées sans ambiguïté.

Ex : qu'est-ce qui est fourni avec une « virtual machine » : vitesse, mémoire, espace disque, usage de tel ou tel logiciel ? chaque prestataire, ou presque, a sa propre réponse! Le périmètre des licences des logiciels associés mérite sur ce point une attention toute particulière.

➢ ***Coûts / Responsabilité***

16. Les services d'intégration avec le reste de mon entreprise / de mon système d'information, sont-ils inclus dans les services envisagés ? Qui les fournit ? Un tiers ? Le prestataire lui-même ? A quel coût ?

Il faut être objectif et intégrer dans le bilan financier du projet l'ensemble des coûts à supporter. Si des tâches d'intégration sont nécessaires (quasiment toujours!), il conviendra d'intégrer ces coûts dans le calendrier du projet et son bilan financier et de se protéger contre les risques de dérapage (forfait…).

Les coûts exposés en cas de dérive due à une mauvaise anticipation des délais et des tâches peuvent se révéler bien plus importants que les services eux-mêmes, il faut en avoir conscience.

➢ ***Coûts / Délais / Qualité / Cloisonnement***

17. Quelle est la mécanique tarifaire du service ?

Ai-je bien compris comment le prix était susceptible de varier selon les hypothèses ? Le projet reste-t-il intéressant dans ces hypothèses ? Comment sont appréhendées les variations de volumétrie ? Est-il prévu des engagements de volume ? de performance ? Quelles sont les conséquences d'une non-atteinte de ceux-ci ?

A défaut d'avoir parfaitement évalué comment ces paramètres sont susceptibles d'impacter mon prix, je risque d'acheter un service mal adapté à mon besoin ou d'être fortement surpris lorsque l'évolution de mon utilisation m'amènera à tester, dans la réalité, les limites de la mécanique tarifaire proposée

➢ ***Coûts***

18. Qu'est-ce qui reste à ma charge en tant que client ?

Autrement dit, qu'est-ce qui n'est pas inclus dans le service ? Qu'est-ce que je n'achète pas ? Il faut « rendre explicite les non-dits » et interpeller le fournisseur sur son obligation de conseil.

➢ ***Coûts / Qualité***

19. Comment les services évoluent-ils dans le temps ?

Cloud rime souvent avec « standard » : le service va donc évoluer avec l'évolution du produit. Quel contrôle puis-je garder sur ces évolutions ? (les refuser ? - n'y pensons pas, dans bien des cas!) Quels seront les impacts de ces évolutions sur les interfaces ? Comment suis-je informé de ces évolutions ?

➢ ***Pérennité***

Engagements de service

20. Quels sont les engagements de service ?

Attention, si les services sont standardisés, les engagements de service le sont aussi. Ces engagements sont-ils réellement significatifs pour moi ? (ex : disponibilité du service exprimée en pourcentage et temps de restauration du service). Permettent-ils réellement de garantir la performance et la qualité du service de bout en bout ? Des indicateurs sont-ils définis - sont-ils pertinents ? - pour assurer un suivi de la qualité de service ? Ces indicateurs font-ils l'objet d'un reporting ?

Un prestataire qui n'intervient que sur la dernière partie de la chaîne, en offrant par exemple une solution SaaS, mais qui se repose sur des prestataires tiers pour assurer l'hébergement de son offre sera nécessairement contraint par les niveaux d'engagement qu'il a lui-même obtenus. L'obtention d'une réelle qualité de service de bout en bout suppose une bonne appréhension des différents intervenants et de leurs responsabilités respectives.

➢ ***Qualité / Performance / Responsabilité***

21. Comment est assurée la continuité du service en cas de sinistre (au sens large) ?

Comment le prestataire assure-t-il une continuité technique et opérationnelle / organisationnelle / administrative en cas de survenance d'un sinistre majeur ? Dans quel délai ? Des tests sont-ils prévus ? Un audit est-il possible ? Comment suis-je moi-même préparé en cas de sinistre ?

Seule une bonne appréhension des risques en amont, notamment en élaborant un plan de continuité d'activité avec mon prestataire, me permettra de m'assurer que je ne risque pas de mettre en danger l'existence même de mon entreprise.

➢ ***Sécurité / Conformité***

22. Que se passe-t-il en cas de non-respect de ces engagements ?

Comment est traité le cas de défaillance du service ? Quelle procédure d'escalade ? Quelles sont les conséquences en cas de défaillance ? ex : pénalités, possibilité de sortie anticipée du contrat. Ces modalités sont-elles adaptées à mon cas particulier ? Dans quelles conditions (notamment coûts et délais) puis-je sortir si la défaillance persiste ?

Les risques associés à une mauvaise appréhension de cette question sont nombreux et susceptibles d'impacter indifféremment les coûts du projet, les délais de réalisation ou de remédiation, la qualité de service - et derrière celle-ci, la qualité de mon propre service à mes propres clients - et, enfin, la sécurité de l'ensemble.

➢ ***Coûts / Responsabilité / Qualité***

Mise en œuvre du service

23. Qui s'engage à mettre en œuvre le service ? selon quel calendrier ?

Qui pilote la mise en œuvre du projet ? Selon quelles modalités et avec quels engagements (respect des délais, du budget, fourniture des livrables…) ?. Quelle procédure de recette pour m'assurer de la conformité de la solution mise en œuvre ?

Une mauvaise appréhension de ce volet se traduira immanquablement par une dérive des coûts et des délais de réalisation.

➢ ***Responsabilité / Coûts***

24. Une fois le service opérationnel, les mêmes questions que dans le cas de prestations classiques se poseront :

Comment signaler un incident ? Par qui est-ce traité ? (ex : quel outil, quel process, quelle langue, quelle rapidité de réaction ?)

✓ Quel reporting et comment est-il fourni ? (ex. portail, via email...)

✓ Comment effectuer une demande de changement ou une demande de service ?

✓ Comment la facturation est-elle effectuée ? Quand et sous quelles conditions payer ?

✓ Quel interlocuteur aurai-je pour la relation contractuelle ? (ex : un site web, un centre d'appel, une personne nommée ?) Qui ai-je nommé pour ce rôle au sein de l'entreprise ?

➢ ***Gouvernance***

25. Quelle gouvernance de la relation sera mise en place ? Qui dans mon organisation s'occupe de la relation avec le prestataire ?

La relation doit être gérée dans le temps. Il convient donc de prévoir le mode de gouvernance adapté, tant à l'entreprise qu'au projet, et s'assurer que les procédures d'escalade idoines permettront de résoudre les difficultés.

➢ ***Gouvernance***

26. Quelles facultés de contrôle / audit ?

Les services de Cloud public sont par définition mutualisés. Il s'ensuit que le prestataire s'opposera généralement à toute possibilité d'audit direct du client, ce qui est légitime au regard de la sensibilité des données de tiers stockées dans ses systèmes. Il faut donc réfléchir aux autres possibilités offertes : contrôle d'un tiers, organisme certificateur, faute de quoi je risque de me trouver dans l'incapacité d'assurer un contrôle interne effectif et, potentiellement, de me mettre en infraction au regard de l'environnement réglementaire applicable à mon activité.

➢ ***Contrôle / Conformité***

27. Quel contrat pour régir mon service ?

Le contrat de services Cloud est bien souvent aussi standardisé que l'offre elle-même. Il s'agit le plus souvent d'un contrat d'adhésion, dans lequel peu de choses sont - apparemment - négociables. Il se concentre également le plus souvent sur la partie service récurrent exclusivement, et omet ainsi d'aborder toute la partie projet.

Or (i) les contrats évoluent et ceux de première génération ne ressemblent déjà plus à ceux qui peuvent être mis en place aujourd'hui, à la suite d'un dialogue constructif autour des problématiques abordées dans ce document et (ii) il n'est pas souhaitable de faire l'impasse, sur le plan contractuel, sur la partie projet, sauf à prendre le risque de se trouver sans aucun référentiel en cas de problème.

Il convient donc d'aborder la question du contrat suffisamment en amont et de s'astreindre à une lecture rigoureuse de celui-ci, afin d'appréhender les points sur lesquels il devrait être aménagé pour mieux répondre aux défis posés.

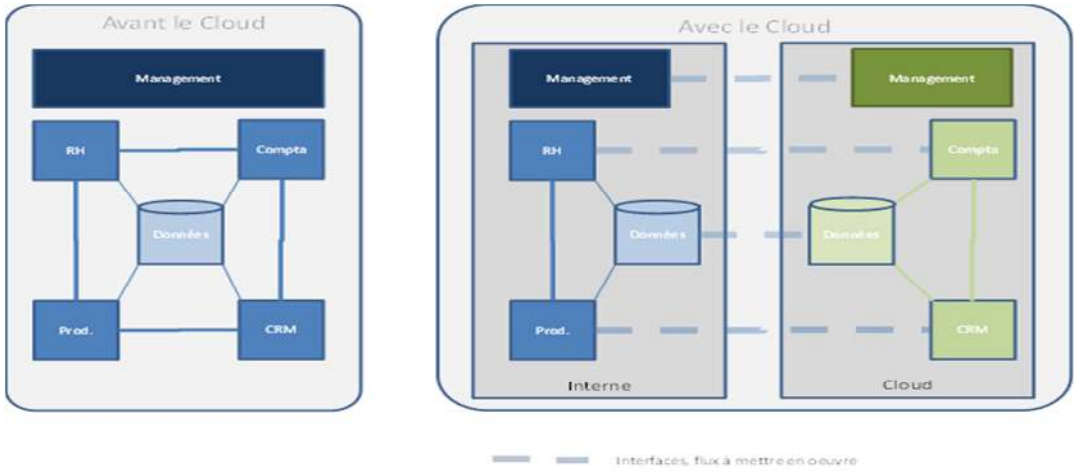
➢ ***Coûts / Sécurité /Conformité / Qualité / Responsabilité***

C. Comment intégrer le Cloud dans mon système d'information ?

Certaines applications sont relativement autonomes et isolées du reste du système d'information. D'autres applications, cependant, sont constituées de plusieurs modules qui fonctionnent sur des environnements techniques différents, qui échangent des nombreux flux d'informations entre eux et avec d'autres applications.

Par ailleurs, des outils de management (monitoring, provisioning, reporting) sont utilisés pour exploiter ces différents modules.

Le schéma ci-dessous illustre la problématique posée par le Cloud en termes d'interfaces/flux à mettre en œuvre.



Interfaces

28. Tous les modules de l'application qui sera mise dans le Cloud peuvent-ils bien être supportés par la plate-forme Cloud du prestataire ?

Il convient non seulement de s'en assurer suffisamment tôt, et le cas échéant de mettre en place les adaptations et interfaces nécessaires, mais aussi de prévoir sur qui repose la responsabilité d'assurer du maintien de cette compatibilité dans le temps, notamment au regard des évolutions respectives de la plate-forme Cloud et de mes applications.

➢ ***Pérennité***

29. Interopérabilité : Comment les modules « Cloud » communiqueront-ils avec les modules « non Cloud » de mon SI ? Quels mécanismes de communication et d'échanges, quelles performances ?

Une étude attentive des flux à mettre en place pour assurer la communication de mon nouveau service Cloud avec le reste du SI de mon entreprise, voire avec les autres solutions Cloud mises en œuvre, est indispensable.

Ne pas traiter ces questions en amont, lors de l'étude du projet, c'est à la fois prendre le risque de re-cloisonner l'entreprise sans pour autant en avoir conscience - ce résultat s'impose de lui-même ! - et s'exposer à des retards, surcoûts et déconvenues lors de la mise en œuvre du projet, car il faudra bien, tôt ou tard, les prendre le compte.

➢ ***Qualité / Cloisonnement / Coûts***

30. Comment assurer une homogénéité de sécurité / confidentialité des données ?

Si des données sont cryptées sur la plate-forme Cloud, comment sont gérées les clés et y ai-je accès (question clé notamment pour la réversibilité) ? Comment les flux de données sont-ils sécurisés entre la plate-forme Cloud et mon SI et au sein de cette plate-forme ?

➢ ***Sécurité / Conformité***

Outils

31. Les outils du prestataire (Ordonnanceur / reporting / monitoring) peuvent-ils s'interfacer aisément avec les miens ?

Quels sont les outils du prestataire que je pourrai utiliser pour gérer et suivre mon nouveau service Cloud ? Sous quelles conditions sont-ils mis à disposition ? Des adaptations/interfaces avec mon propre système seront-ils requis ? Ces outils sont-ils inclus dans le coût du service ?

Les réponses à ces questions doivent normalement se trouver dans la proposition du prestataire et le contrat de service Cloud.

➢ ***Coûts / Pérennité***

D. Comment protéger mes données dans le Cloud ?

La problématique des données et de leur protection dans le Cloud est sans doute l'une de celles qui fait couler le plus d'encre. De fait, c'est une problématique clé au regard des enjeux qu'elle représente.

Cela est notamment dû à la nature même du Cloud qui implique une perte de contrôle du client utilisateur sur ses propres données, alors même qu'il en demeure généralement pleinement responsable. C'est en effet en principe sur le client utilisateur que reposent les obligations légales d'assurer la sécurité et la confidentialité de ses données, en tant que responsable de traitement, et non sur le prestataire de service Cloud, simple sous-traitant au sens de la réglementation actuelle. C'est la règle « classique ».

Or, dans le Cloud, les données voyagent, sont copiées, échangées, éclatées, disséminées, parfois dans le monde entier, et ce bien souvent hors du contrôle du client utilisateur. Les services Cloud présentent donc un challenge important sur le plan de la conformité légale, qui requiert d'aller au-delà de la simple affirmation et répétition de la règle classique.

Il s'agit aujourd'hui d'une contrainte majeure, incontournable, encadrée par de multiples obligations légales et réglementaires.

Niveau de sensibilité des Données

Selon le niveau de sensibilité des données, il conviendra de s'orienter vers des prestataires disposant, le cas échéant, des qualifications et agréments nécessaires. De fait, il convient de se poser les questions suivantes :

32. Quelles données sont concernées et quel est leur niveau de sensibilité ?

Toutes les données ne sont pas éligibles au Cloud. C'est la première question à se poser et il est rare que la réponse soit immédiate. Beaucoup d'entreprises sont encore incapables de répondre à cette question sans effectuer des recherches approfondies, qui généreront bien souvent elles-mêmes d'autres questionnements. De fait, le passage au Cloud, en mettant le doigt sur la question des flux de données et de leur protection, force l'entreprise à se poser certaines questions qu'elle avait pu, consciemment ou pas, ignorer jusque là.

Il conviendra de procéder à un recensement précis des divers types de données manipulées dans les applications et bases de données concernées et de déterminer leur niveau de sensibilité au regard des normes applicables (les données sensibles sont celles qui concernent les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales, ou qui sont relatives à la santé ou l'orientation sexuelle des personnes).

A défaut, le risque de non-conformité est patent, et les sanctions prévues par les texte encourues.

➢ ***Conformité***

33. A quelles contraintes réglementaires les données sont-elles éventuellement soumises ?

Au-delà de la sensibilité des données au sens ci-dessus, celles-ci peuvent faire l'objet de contraintes réglementaires spécifiques, selon mon secteur d'activité.

Ainsi, des données de santé, ou des données bancaires, sont soumises à des régimes particuliers et ne peuvent être confiées à n'importe quel prestataire. L'implication de la direction juridique de l'entreprise est ici indispensable pour appréhender les obligations légales qui s'imposent et m'assurer qu'elles trouvent une réponse adaptée dans la solution Cloud que je projette.

➢ ***Conformité***

Localisation des Data Centers

34. Ai-je besoin de savoir où sont mes données ? Si oui, ai-je la réponse du prestataire ?

Le plus souvent, la réponse à la première de ces questions sera oui et la réponse à la seconde, plus difficile à obtenir. Or, en qualité de responsable de traitement, le client utilisateur ne peut faire l'impasse sur cette question, comme l'illustre la suite de ce chapitre.

➢ ***Conformité / Contrôle***

35. Est-ce que mes données sont transférées hors de l'UE ou d'un pays ayant un niveau de protection reconnu adéquat ?

Le transfert de données hors de l'union européenne ou d'un pays ayant un niveau de protection reconnu adéquat est soumis à des contraintes particulières.

Je dois donc impérativement savoir si c'est le cas, sous peine de me mettre en infraction.

➢ ***Conformité / Contrôle***

FOCUS - PROTECTION DES DONNÉES PERSONNELLES
LES RECOMMANDATIONS DE LA CNIL
EN MATIÈRE DE CLOUD

Dès lors que des données à caractère personnel seront confiées et/ou transférées au prestataire Cloud, la loi Informatique et Libertés impose des contraintes à la charge principale du client utilisateur des services, mais également à la charge du prestataire Cloud. La première de ces contraintes est d'assurer la sécurité et la confidentialité des données appréhendées par le service Cloud. La CNIL encourage les entreprises, et donc les métiers concernés, à se poser les bonnes questions sur la protection des données avant d'externaliser dans le Cloud.

En juin 2012, dans le prolongement d'une consultation publique sur le Cloud, la CNIL a ainsi émis des recommandations qui visent à aider les entreprises françaises à prendre des décisions éclairées lors du recours à un service Cloud (1). Ces recommandations, très concrètes, visent à permettre aux clients utilisateurs de services Cloud d'anticiper les risques en matière de protection des données personnelles. Elles contiennent notamment une liste détaillée des « Eléments essentiels devant figurer dans un contrat de prestation de services de Cloud Computing » qui identifie, entre autre, les informations relatives aux traitements qu'il échoit au prestataire de ce type de services de fournir, les garanties qu'il doit mettre en œuvre en matière de conservation, destruction et/ou restitution des données et les exigences de sécurité à respecter. Le tout est accompagné de modèles de clauses pouvant être utilisées dans ces contrats.

1(http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf)

Sécurité des données

Si je suis responsable de la sécurité des données que je confie à un prestataire, j'ai intérêt à m'assurer que celui-ci traitera mes données avec toutes les mesures de sécurité nécessaires, notamment pour en assurer l'intégrité, la confidentialité, l'imputabilité et leur disponibilité. Ces mesures seront d'ordre logique (anti-virus, gestion des droits d'accès en fonction des profils, séparation logique entre 2 Virtual Machines) et d'ordre physique (surveillance vidéo des data centers, climatisation…).

D'où les questions suivantes :

36. Quels sont les dispositifs physiques et logiques de sécurisation des données mis en œuvre ?

Ces dispositifs devront être recensés avec soin dans le contrat, évalués et validés au regard des obligations légales applicables compte tenu de la nature des données et garantis par le prestataire.

➢ ***Conformité***

37. Quels sont les moyens de traçabilité / audits disponibles ?

Il conviendra de pouvoir s'assurer, de manière proactive et réactive, que la sécurité des données est bien assurée. D'où la nécessité de prévoir des moyens d'audit et de

s'assurer que la traçabilité des accès aux données est bien assurée.

➢ ***Contrôle***

38. Ces moyens sont-ils étendus aux éventuels sous-traitants ?

La sécurité des données est illusoire si la chaîne de sécurité est rompue. Si des sous-traitants sont prévus (d'où l'importance d'aborder cette question en premier lieu), il conviendra de s'assurer qu'ils sont pleinement intégrés dans les dispositifs de sécurité mis en œuvre et que le prestataire en répond.

➢ ***Contrôle***

39. Quelles sont les modalités de notification des failles de sécurité ?

Si je dois moi-même alerter les intéressés dont je détiens des données en cas de faille de sécurité (cette obligation existe déjà dans certains pays / domaines d'activité et est en passe d'être généralisé en Europe, il est essentiel que je sois informé en temps et en heure si cela se produit. Il est donc légitime que j'obtienne des engagements forts de mon prestataire sur ce point.

➢ ***Responsabilité***

FOCUS Le Guide sécurité de l'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié un guide intitulé « Maitriser les risques de l'externalisation », qui pourra utilement être consulté sur les problématiques sécurité liées aux opérations d'externalisation et notamment au Cloud Computing (http://www.ssi.gouv.fr/externalisation).

L'ANSSI identifie notamment les risques liés :

- à la confidentialité des données ;
- à l'incertitude sur la localisation des données (en particulier pour les données à caractère personnel, le patrimoine scientifique et technique) ;
- à la perte de maîtrise du système d'information (forte dépendance au prestataire quant aux choix techniques, incapacité à déceler et gérer les incidents) ;
- à la mutualisation des ressources (isolation défaillante des données et effacement incomplet de celles-ci).

Le guide propose une démarche reposant sur la rédaction d'un Plan d'Assurance Sécurité (PAS), pour apprécier les risques et fixer les exigences en fonction du contexte de l'opération, afin de garantir la sécurité des systèmes d'information et des données qu'ils traitent. Il fournit également certaines clauses types utiles.

40. Assurances : ai-je pris les précautions nécessaires ?

Ma police RC / Exploitation couvre-t-elle mon évolution vers le Cloud ? Ai-je souscrit une assurance particulière pour me protéger contre les risques de perte, de piratage ou de contamination de mes données ?

➢ ***Coûts / Responsabilité / Pérennité***

E. Ai-je bien les droits de faire ce que je souhaite faire avec le Cloud ?

Les Services Cloud s'appuient sur de nombreux logiciels mis en œuvre par les Prestataires Cloud. Dans ce cas, il est nécessaire de s'assurer que le client utilisateur disposera bien des droits requis pour utiliser ces logiciels. D'autre part, si le service est de type PaaS ou IaaS, il conviendra de s'assurer que les licences dont dispose le client utilisateur permettent leur utilisation sur la plate-forme du prestataire.

Ces situations justifient que l'on se pose certaines questions et que les responsabilités soient bien réparties entre les parties :

Responsabilité du Prestataire

41. Le prix des services couvre-t-il bien l'utilisation de tous les logiciels utilisés/mis à disposition par le prestataire dans le cadre des services ?

C'est normalement le cas et ce doit l'être. Le client utilisateur ne dispose en effet d'aucun moyen propre de s'assurer qu'il a acquis toutes les licences requises. Ce principe doit rester vrai pendant toute la durée des services Cloud, quelles que soient les évolutions enregistrées.

➢ ***Coûts / Responsabilité***

42. Le prestataire garantit-il que les logiciels qu'il met à ma disposition ne contreviennent pas aux règles de Propriété Intellectuelle ?

A nouveau, seul le prestataire est en mesure de donner cette garantie et il est essentiel au client utilisateur de l'obtenir, pour s'assurer qu'il ne sera pas gêné dans son usage des services Cloud.

➢ ***Responsabilité***

43. Le prestataire me garantit-il contre toutes les conséquences d'une réclamation d'un tiers sur cette question ?

C'est le corollaire normal du point précédent. A défaut, le client utilisateur peut se trouver en situation de devoir

payer à nouveau, cette fois-ci au détenteur des droits, pour l'utilisation de la plate-forme.

➢ ***Responsabilité***

Mes responsabilités

44. Pour les logiciels que je vais installer sur une infrastructure Cloud (typiquement les applications), est-ce que je dispose bien des licences adéquates ?

Ce point n'est pas toujours évident et une vérification attentive des conditions de licence s'impose donc, que seule peut faire le client utilisateur. Le prestataire sera fondé, pour sa part, à demander une garantie réciproque de celle qu'il donne lui-même, que les logiciels utilisés par le client utilisateur sur sa plate-forme Cloud n'enfreignent aucun droit de propriété intellectuelle.

➢ ***Coûts / Responsabilité***

45. De quels moyens de reporting puis-je disposer pour m'assurer que je sais suivre en permanence l'utilisation que je fais de ces logiciels ?

Il convient de m'assurer que je dispose des outils d'administration appropriés pour suivre cette utilisation. A défaut, il conviendra d'obtenir du prestataire qu'il le fasse pour moi et m'en rende compte.

➢ ***Gouvernance / Contrôle***

F. Comment rentrer dans le Cloud et en sortir ?

Ceux qui ont fait le choix de souscrire à un service Cloud doivent également considérer la portabilité de leurs traitements vers et depuis l'écosystème Cloud au même titre que la récupération de leurs données et leur destruction.

Les prestataires proposant des services Cloud ont axé leurs discours sur la flexibilité à pouvoir augmenter ou réduire rapidement les ressources de calcul et de stockage disponible pour un service Cloud. On devrait y ajouter l'interopérabilité, tant il est vrai qu'à terme, tous les services, produits, logiciels, matériels, utilisés par l'entreprise doivent pouvoir communiquer entre eux.

Les clauses de réversibilité, de destruction des données, de capacité d'audit et d'interopérabilité[1] des écosystèmes présentent par conséquent un enjeu essentiel.

Pouvoir accéder à ses données/applications au fil du temps, indépendamment de la technologie utilisée par le prestataire et pouvoir assurer leur portabilité vers un autre prestataire sont des questions critiques qui doivent obtenir une réponse précise avant de s'engager.

On se posera, à cet égard, utilement, les questions suivantes :

Migration vers le Cloud

46. Comment porter mes applications vers la plate-forme ?

Si je transporte des applications que j'utilise déjà actuellement vers le Cloud, c'est à une véritable migration que je suis confronté. Ce type de projet ne s'improvise pas : Qui la pilote ? Qui me conseille ? Qui teste avant sa mise en œuvre ? S'il s'agit de nouvelles applications, c'est en outre d'une transformation qu'il s'agit et qui devra donc être soigneusement préparée.

➢ ***Responsabilité***

47. Comment porter mes données vers la plate-forme ?

C'est d'un véritable chantier de migration de données que l'on parle ici. Quel format utiliser ? Quel moyen (transmission électronique ou livraison physique des supports de données) ? Quelle quantité de données ? Quels délais ? Quel pilote ? Comment s'assurer de l'intégrité des données transférées ? Quels tests ? Tout cela doit être anticipé, traité et formalisé.

➢ ***Coûts / Responsabilité***

48. Les coûts de migration ont-ils bien été identifiés et inclus dans le calcul du retour sur investissement ?

A défaut d'avoir identifié ces coûts en amont, je risque de mauvaises surprises lorsqu'il s'agira de vérifier le ROI de mon projet. Qui me conseille ? Quel est l'engagement de mes divers prestataires sur ces coûts ? Qu'est-ce qui est pris en charge et qu'est-ce qui reste à ma charge ?

➢ ***Coûts / Responsabilité***

Réversibilité - migration depuis le Cloud

49. Comment récupérer les données, les applications ? Quel format de restitution des données (format libre, format du marché) ? Mon prestataire est-il certifié ?

Au-delà des questions de format des données - il est indispensable de récupérer les données dans un format qui puisse être lu par les applications standards du marché - et des problématiques inverses de celles déjà examinées s'agissant de la migration vers le Cloud, la question de la mise à disposition des outils nécessaires pour assurer la récupération des données et des délais et coûts correspondants doit également être abordée.

La question n'est pas anodine et suscite encore une réelle interrogation tant il est vrai que le manque de standardisation des applications (et donc des formats) complique les choses en rendant bien souvent indispensable le développement d'API ou de « connecteurs » pour assurer l'interopérabilité et la réversibilité des données.

[1] Interopérabilité : ensemble du matériel et des logiciels qui permettent à un système composé d'équipements hétérogènes de réaliser un travail commun

A cet égard, il est particulièrement intéressant de noter que la 1ère jurisprudence française en matière de Cloud a récemment mis l'accent sur la nature de l'obligation du prestataire de services Cloud au regard de la récupération des données, n'hésitant pas à qualifier de « Contrat d'intérêt commun » le contrat de Cloud, pour imposer au prestataire le maintien des services tant qu'il n'a pas mis à disposition de son client un moyen fiable lui permettant de récupérer l'ensemble de ses données (affaire Oracle c. UMP).

Également à suivre, le développement de la certification qui, en traitant la question de la réversibilité, permet de s'assurer que l'on traite avec un prestataire disposant d'un standard d'export compatible avec les principaux standards du marché.

Afin d'éviter toute déconvenue en fin de contrat, cette capacité à récupérer les données devra être testée dès que possible.

➢ ***Pérennité / Responsabilité / Coûts***

50. Les coûts de la réversibilité sont-ils chiffrés ?

Attention aux mauvaises surprises ! C'est au montage du projet qu'il convient de s'assurer que l'on pourra en sortir en cas de besoin, et d'en préciser alors les conditions, notamment financières. Qui supportera les coûts de la migration des données ? Qui sera responsable si elle ne peut intervenir et dans quelles limites ?

➢ ***Coûts***

51. Comment obtenir la destruction des données, après la fin du contrat ?

Puis-je être sûr que toutes mes données, une fois récupérées sur mes systèmes (ou ceux de mon nouveau prestataire), seront effacées des systèmes du prestataire ? Il conviendra de s'en assurer et d'obtenir les garanties et moyens de contrôle correspondants dans le contrat.

➢ ***Sécurité / Contrôle***

Conclusion

Au fil de ces questions, on perçoit que derrière la facilité apparente des solutions Cloud, le montage d'un projet Cloud nécessite une vraie réflexion stratégique et une bonne concertation avec les fonctions transverses de l'entreprise : DSI, RH et juridique notamment.

Le Cloud n'a pas vocation à faire prendre des risques à celui qui le met en œuvre, mais c'est pourtant toute une quantité de nouveaux risques qui se présente à la porte de celui qui se lance dans ce type de projet, qu'il convient par conséquent d'identifier et de gérer avec soin, sous peine qu'ils se matérialisent. Le Cloud n'a pas plus vocation à cloisonner l'entreprise, mais c'est pourtant ce qu'il peut faire, et de façon très puissante, si on ne se préoccupe pas suffisamment tôt de bien l'intégrer au sein de l'entreprise et d'assurer son interopérabilité effective avec le SI et les autres solutions/applications et données de l'entreprise.

Il n'y a qu'à imaginer ce qui pourrait se passer dans une entreprise dans laquelle chaque métier monterait sa solution Cloud propre, sans se soucier des autres métiers, ni des fonctions transverses, ni des systèmes existants… On arriverait rapidement au syndrome de la tour de Babel, caractérisé par l'impossibilité des uns et des autres à communiquer ensemble !

Il n'est cependant pas facile de bien faire les choses, car les questions posées sont complexes et les directions concernées ne disposent pas toujours des compétences nécessaires, que ce soit en interne ou dans les fonctions transverses. De fait, il faut reconnaître que le Cloud requiert de nouvelles compétences et pousse vers la création de nouveaux métiers au sein de l'entreprise, capables d'intégrer les multiples dimensions de ces projets et de leur faire générer tout leur potentiel de libération de valeur.

De fait, à l'heure du Big Data, alors que l'on découvre à peine le potentiel de création de valeurs que recèle l'exploitation des nombreuses données accumulées par l'entreprise, qui pourrait prendre, sans risquer de la regretter amèrement très vite, la décision de monter tout seul son projet Cloud, en faisant l'impasse sur le reste de l'entreprise ?

Il convient donc d'être vigilant et de mener en amont la réflexion et la concertation nécessaires. Alors seulement, pourra-t-on bénéficier pleinement des possibilités gigantesques offertes par le Cloud, lorsqu'il est bien pensé !

* * *

REMERCIEMENTS

Ce billet a vu le jour grâce à la motivation et à la participation des membres de la Commission Juridique de l'EOA, et notamment

PERRINE BOITEAU
Orange

JACQUES LANNEFRANQUE
Crossbird

BERTRAND CASAMITJANA
Thales

LAURENT MICHON
Atos

David CHARLOT
Suez Environnement

JEAN-MICHEL PETIN
Nitep Consulting

PIERRE DELECOURT
Verizon

ELODIE POMMEPUY
Steria

Je les en remercie vivement

RÉMY BRICARD
Président de la Commission Juridique, EOA France
Avocat Associé, Baker & McKenzie Paris