Cahiers Techniques | 2014

COMMISSION | SYSTEMES D'INFORMATION

Cloud Computing

Les questions clés que doivent se poser les Risk Managers

En partenariat avec

solucom
management & IT consulting

AMRAE
ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE

L'AMRAE tient à remercier les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

François BEAUME	Président de la Commission SI de l'AMRAE, Directeur du Risk Management - Dalkia
Alain GRAVIER	Risk Manager – FDJ (La Française des Jeux)
Gérôme BILLOIS	Senior Manager - Practice Risk Management - Solucom
Garance MATHIAS	Avocat à la Cour
Mickael ROBART	Directeur-Siaci Saint Honoré
Hélène DUBILLOT	Directeur Coordination Scientifique - Amrae

Avant-propos

Le Cloud, tout le monde en parle et c'est un des sujets d'actualité en matière de risque numérique.

Pour appréhender les enjeux de cette (r)évolution fondamentale des systèmes d'information de l'entreprise, nous avons souhaité réunir plusieurs spécialistes venus d'horizons différents (Risk Managers, Expert SI, avocat, courtier en assurances), afin qu'ils puissent diffuser leur connaissance et leurs réflexions aux membres de l'AMRAE et ainsi délivrer aux Risk Managers les clés d'une meilleure compréhension de cette technologie.

Dimension stratégique, nouveaux risques, cadre juridique et aspects assurantiels, sans oublier le point de vue du Risk Manager, tels sont les points abordés dans ce cahier technique qui se veut avant tout pragmatique, utile et instructif pour les membres de l'AMRAE.

Nous vous en souhaitons une excellente lecture, et nous espérons que cette nouvelle publication alimentera vos réflexions et vous permettra d'optimiser vos pratiques sur ce sujet dans vos organisations.

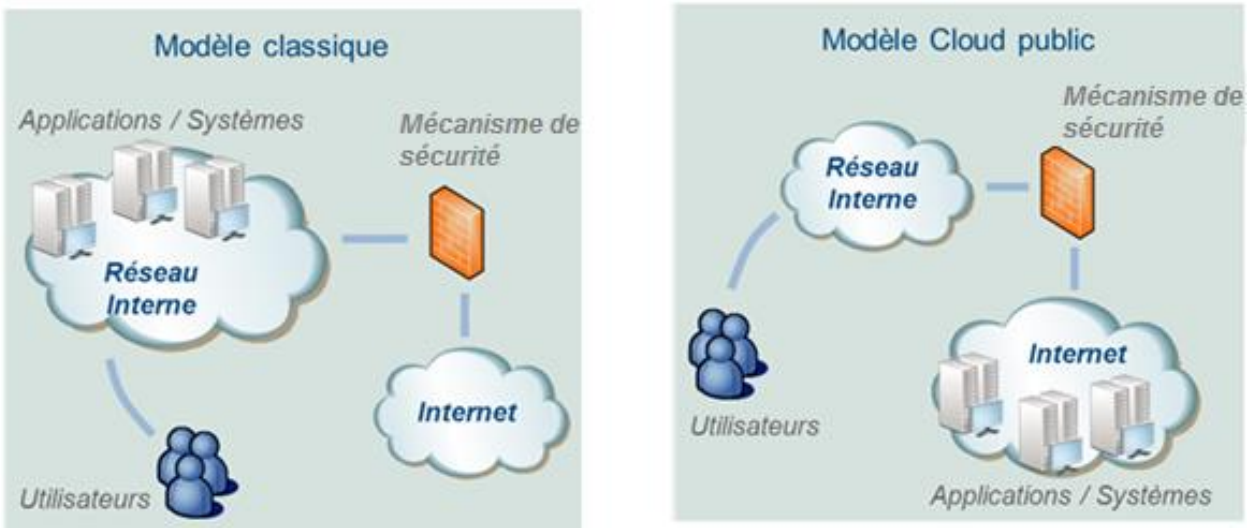
François Beaume, Président de la Commission Systèmes d'information de l'AMRAE

Table des matières

I - Cloud computing : démystification

1. Qu'est-ce que le cloud computing ?

Le cloud computing est une évolution fondamentale des systèmes d'informations. Le modèle classique, avec un SI interne sur lequel sont situées les ressources informatiques (applications, systèmes…), se transforme en un modèle cloud où les applications et les systèmes sont mutualisés et peuvent être hébergés sur Internet.



Evolution d'un modèle classique vers un modèle de cloud public

Le terme cloud computing inclut des mises en œuvre différentes, le cloud privé et le cloud public.

Le cloud privé est construit sur mesure par l'entreprise. La DSI produit un cahier des charges, le fait réaliser et possède un contrôle total sur le cloud. Il y a peu d'évolution des risques car la situation reste proche du modèle de départ : le système est maîtrisé et connu de la DSI.

Le cloud public correspond aux offres industrialisées disponibles sur Internet. L'entreprise souscrit à des services directement en ligne, parfois aussi simplement que pour acheter un bien marchand. Le service est hébergé sur Internet par un tiers, il est mutualisé potentiellement avec d'autres clients. La DSI contrôle donc moins le système. De nouveaux risques apparaissent.

Il existe plusieurs services dans le cloud, dont :

- **Des applications : « Software As A Service » (SaaS)**
  Exemples : *messagerie, gestion de la relation client CRM, gestion des commandes…*
- **Des infrastructures : « Infrastructure As A Service » (IaaS)**
  Exemples : *serveurs, réseaux, sauvegardes…*

- **Des environnements de développement et d'exécution d'application : « Platform As A Service » (PaaS)**
  Exemples : *Amazon EC2, Microsoft Azure, Google App Engine*

Les acteurs du cloud proposent des services qui peuvent s'adresser à la fois aux professionnels et aux particuliers. Des poids lourds du secteur, comme Google et Microsoft se sont d'ailleurs construits sur des offres grand public, qu'ils ont ensuite ouvertes aux professionnels.

2. Quelles sont les promesses du cloud computing ?

Les services de cloud sont rapides à mettre en place. Le modèle de cloud public permet d'acheter, de configurer et de mettre à disposition des utilisateurs une application en quelques heures, là où jusqu'à présent, il était nécessaire d'acquérir les différents composants pour construire l'application. Les délais de mise en place étaient considérables et pouvaient se compter en mois.

Le cloud permet une facilité d'accès aux services, souvent par Internet. Les collaborateurs en situation de mobilité ou se déplaçant sur les sites de l'entreprise en sont les premiers bénéficiaires.

Le cloud porte une promesse de réduction des coûts. En effet, la facturation se fait à l'usage, au plus près de la consommation : l'utilisateur paye pour ce qu'il consomme réellement. D'autre part, l'industrialisation des services permet une réduction de leurs coûts. Enfin, le modèle, souple, s'adapte presque en temps réel à la demande, contrairement au modèle historique de la DSI basé sur des investissements par paliers. Les investissements diminuent donc au profit de coûts de fonctionnement. Cependant, toutes ces promesses ne sont pas toujours atteintes. L'expérience montre que des études sont nécessaires pour les valider.

3. Quels changements au quotidien ?

Le cloud modifie souvent le degré de connaissance et de spécialisation des systèmes utilisés. Dans le modèle classique, l'entreprise fait construire son propre système selon ses spécificités. Dans le modèle du cloud public, elle achète une offre industrialisée avec des possibilités de spécialisation moindres. De plus, les fournisseurs protègent leurs innovations en communiquant peu d'informations sur le fonctionnement de leurs services, sur l'emplacement des différents éléments, sur le dimensionnement de leurs équipes, sur l'architecture utilisée… L'entreprise a donc des difficultés à savoir comment le système fonctionne et quels sont les risques inhérents.

Le passage d'un modèle classique à un modèle cloud fait fondamentalement évoluer le rôle de la DSI et soulève des problématiques de ressources humaines. Aujourd'hui, la majorité des DSI disposent de compétences techniques et conçoivent des systèmes entiers. Avec le cloud, la DSI devient un acheteur, un assembleur et un distributeur de services. Le besoin en connaissances techniques très pointues diminue au profit de compétences dans le domaine des achats, de la gestion des fournisseurs, de la relation client avec les métiers…

4. Comment se structure le marché du cloud ?

Le marché du cloud est segmenté entre des acteurs internationaux (Google, Amazon, Salesforce…) et locaux (clouds souverains, fournisseurs français : OVH, Gandhi, Orange…). Leur positionnement varie selon qu'ils fournissent une offre complète et large de service ou des solutions pointues, centrées sur un métier. Les niveaux de maturité sont aujourd'hui très variables entre les différents acteurs.

II - Évolution des risques dans le cloud

1. Une relation fournisseur modifiée

A. Augmentation des fournisseurs

Du fait de l'utilisation des services du cloud, simples à mettre en œuvre, **les fournisseurs se multiplient**. Chaque métier peut aujourd'hui trouver l'application qui couvre parfaitement son besoin, le plus souvent de manière très verticale. Cependant, l'entreprise a besoin que ces applications communiquent ensemble. L**'interconnexion** entre ces systèmes est toujours compliquée voire parfois impossible. Ceci entraîne l'apparition de nouveaux **risques d'incohérence globale du système d'information**.

Le moyen de couvrir ces risques est d'impliquer systématiquement la DSI dans l'ensemble des projets liés au cloud afin qu'elle assure la cohérence entre les différents systèmes pour permettre à l'information de circuler au sein de l'entreprise.

B. Disponibilité des services

Les fournisseurs de cloud computing mettent fréquemment en avant l'infaillibilité de leurs services, qui reposent sur Internet. Ils ne manquent d'ailleurs pas d'utiliser cette caractéristique comme un argument marketing.

Cette infaillibilité n'existe que théoriquement… **des incidents surviennent**, même chez les plus grands fournisseurs de cloud comme Google ou Amazon.

On constate en outre l'apparition **d'effets d'amplification**, comme ce fut le cas pour Amazon en août 2012, qui a connu une panne importante de ses services. La panne a touché les clients directs d'Amazon mais aussi les clients indirects. Sur son cloud, Amazon hébergeait les services d'autres entreprises, comme Instagram, AirBnB ou encore Pinterest, dont les utilisateurs ont perdu l'accès aux services du fait de la panne.

Il existe à terme **un risque systémique** : si un de ces fournisseurs majeurs du cloud tombe, **un effet domino** risque de se déclencher. Il est important pour l'entreprise de savoir si le prestataire avec lequel elle contracte repose sur un autre fournisseur.

Cependant, cette **évolution des risques par rapport à la disponibilité des SI doit être relativisée.** Les SI internes des entreprises ne sont pas exempts de défauts : les incidents sont fréquents - bien que moins médiatisés.

2. Vis-à-vis des cybercriminels

L'évolution vers le modèle de cloud a également fait évoluer la cybercriminalité. Le cloud intéresse les cybercriminels car il permet le **« Crime As A Service »** : les cybercriminels utilisent la puissance du cloud pour réaliser leur méfait, en y hébergeant certains de leurs services d'attaque. Ils bénéficient d'une puissance décuplée.

Le cloud concentre les informations de beaucoup d'entreprises: si un cybercriminel arrive à corrompre le SI d'un fournisseur, il peut potentiellement pénétrer le SI de toutes les sociétés présentes sur ce cloud. C'est le principe du **« break one / break all ».**

Ce dernier risque est cependant à relativiser. La sécurité est en effet cruciale pour la majorité des fournisseurs, dont la fourniture de services informatiques est le cœur de métier. Chez la majorité des fournisseurs, le niveau de sécurité est supérieur à que ce qu'on peut trouver dans les entreprises. Ils le prouvent grâce à l'obtention de certifications et grâce aux audits qu'ils réalisent.

3. Vis-à-vis des autres États et de l'intelligence économique

Les Etats ont un intérêt très fort pour le cloud computing car il concentre beaucoup d'informations et donne des capacités d'analyse très intéressantes ! Les récentes révélations sur les écoutes de la NSA ont mis en lumière cet intérêt étatique.[1]

Le droit au respect de la vie privée et à la protection des données sont des droits fondamentaux protégés par le droit de l'Union européenne, notamment en application des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Si l'Union européenne protège ce droit, il convient de noter que **la Constitution des États-Unis ne mentionne pas explicitement un droit au respect de l'intimité**, alors qu'aujourd'hui la majorité des grands fournisseurs sont anglo-saxons.

En outre, aux États-Unis, il faut préciser que **le *Patriot Act*,** loi fédérale américaine adoptée le 26 octobre 2001 (prorogée et révisée à plusieurs reprises) a modifié certaines dispositions américaines existantes, notamment le *Foreign Intelligence Surveillance Act* (dit *FISA Act*) et le régime des courriers de sécurité nationale (*National security letter*) que nous aborderons plus particulièrement.

Il convient toutefois de garder à l'esprit que d'autres mécanismes, plus traditionnels, existent pour obtenir des informations comme les mandats de perquisition (*search warrants*) ou les sommations de communiquer (*grand jury subpoenas*).

L'objectif du législateur américain était de faciliter la collecte des données personnelles par certaines autorités d'investigation américaines (le FBI par exemple), y compris celles des citoyens européens.

[1] Ces écoutes sont possibles juridiquement

Les autorités américaines peuvent donc solliciter la communication de données détenues par des entreprises européennes, notamment pour motif de lutte contre le terrorisme.

Avant l'adoption du *Patriot Act*, le *FISA Act* permettait déjà au FBI de solliciter, auprès d'une cour de justice spéciale, une ordonnance (appelée *FISA Order*) obligeant des tiers à communiquer des documents « commerciaux » pour les besoins des services de renseignement ou dans le cadre de la lutte contre le terrorisme. Cependant, ces documents étaient limités aux locations de voiture, d'hôtel, d'entrepôts et aux transports en commun.

Désormais, il est possible pour le FBI d'obtenir une ordonnance imposant à un tiers la communication de tout élément tangible pour les besoins d'une enquête liée au terrorisme ou aux activités clandestines de renseignement. Dès lors, les données se trouvant dans le cloud computing peuvent faire l'objet d'une telle ordonnance.

Parmi plusieurs dispositions pouvant être considérées comme attentatoires au respect de la vie privée ou au secret des affaires, celle relative à « l'ordre de bâillonnement » (*« gag » order*) est particulièrement débattue. En effet, cet ordre empêche la personne ayant reçu un *FISA Order* de divulguer toute information quant à cette procédure. A titre d'illustration, un prestataire cloud ne serait pas en mesure d'informer ses clients qu'il a transmis des données leur appartenant au FBI.

Le FBI préfère utiliser la procédure des *National security letter* (*NSL*), plus simple à mettre en œuvre et ne nécessitant pas l'autorisation d'une cour de justice. Il s'agit en effet d'une sorte d'injonction administrative que le FBI et d'autres agences gouvernementales américaines peuvent utiliser pour obtenir certains documents et renseignements relatifs à différents types d'enquêtes gouvernementales. Le Patriot Act est venu étendre les pouvoirs du FBI qui a notamment accès à tous les dossiers des crédits à la consommation. On retrouve également le « gag » order dans cette procédure. Cependant, les dispositions concernant les *NSL* limitent l'étendue des données pouvant être communiquées par les fournisseurs de service Internet, à savoir les noms de leurs clients, leurs adresses et le temps de connexion.

Dès lors, s'il est concerné, l'utilisateur du cloud doit s'attendre à ce que son prestataire respecte les lois américaines, il peut parfaitement lui demander de communiquer les données de manière raisonnée. Ainsi, il est possible de prévoir dans le contrat que le prestataire cloud s'engage à communiquer le minimum demandé par les autorités américaines.

Il y a donc une évolution du risque sur la confidentialité. Néanmoins, **ce risque doit aussi être relativisé** car il est corrélé aux informations et aux services présents dans le cloud. Avant l'envoi de documents sensibles de la DG, de secrets industriels ou d'applications critiques pour l'entreprise dans le cloud, une analyse de risque sera nécessaire.

4. Vis-à-vis des risques juridiques

Le cloud computing englobe de nombreux enjeux, notamment ceux du contrôle, de la sécurité et de la traçabilité des données. Le contrat de cloud devra avant tout fixer les frontières de la responsabilité de chacun.

Dès lors, à l'occasion des négociations et de la rédaction du contrat, il sera nécessaire de soulever notamment :

La question de l'obligation de conseil de la part du prestataire. Il s'agit là d'une obligation qui va plus loin que les simples obligations d'informations ou de renseignement. Les clients doivent en effet pouvoir être renseignés sur leurs besoins réels qu'ils soient novices ou spécialistes. Il faut ainsi souligner que le prestataire se doit de livrer autant les informations que les outils nécessaires aux besoins de son client. Cette obligation de transparence s'applique également à l'information relative à la localisation des données.

La question de l'obligation de collaboration du client. Véritable corollaire à l'obligation de conseil du prestataire, la collaboration consiste en ce que le client exprime ses besoins réels et prenne connaissance des solutions et des services proposés par le prestataire.

La question de la confidentialité et de la sécurité. Tous les savoir-faire, résultats, informations sur des clients ou **données à caractère personnel** (notamment les données bancaires ou médicales) doivent être sécurisées et ne pas être divulguées. Dans le cas de ces dernières, le client devra prendre en considération les garanties offertes par le prestataire cloud pour leur protection. Il est par ailleurs important de prévoir que le prestataire cloud fournira au client toutes les garanties nécessaires au respect de ses obligations au regard de la loi Informatique et Libertés, notamment en termes d'information des personnes concernées, d'encadrement des transferts et de sécurité des données.

De manière globale, il reviendra au prestataire d'assurer la confidentialité des données qui lui sont confiées et d'indemniser le client dans le cas où son service aura été défaillant. Il sera également nécessaire de délimiter strictement les cas de force majeure (à titre d'illustration, un prestataire peut souhaiter inclure les pannes de réseaux, d'électricité, etc.). De même, une clause prévoyant l'obligation pour le prestataire de cloud de contracter une assurance pourra s'avérer intéressante en cas de pertes d'exploitation pour le client.

La question de la clause de propriété intellectuelle. La titularité des droits de propriété devra être clairement précisée dans le contrat. De même, il sera nécessaire d'intégrer une clause de cession des droits de propriété sur les développements spécifiques éventuellement réalisés par le prestataire pour les besoins de l'entreprise décidant de recourir au cloud.

La question de la mise en place d'une clause de réversibilité. Cette clause occupe sans nul doute une place majeure dans un contrat cloud. Le but est de prévoir la possibilité de revenir à une situation antérieure et donc de pouvoir récupérer les données au cas où il y a une défaillance de la part du prestataire ou lorsque le client souhaite changer de prestataire.

La question de l'interopérabilité. Cette clause est très liée à la réversibilité : le changement de prestataire peut en effet être rendu difficile du fait des architectures différentes utilisées par ces derniers. Le but d'une telle clause est d'assurer que les données soient transférables à un autre prestataire, par exemple en utilisant un format commun par exemple.

La question de la clause de Service Level Agreement (SLA). Cette clause est pour le client « la garantie ultime » que le prestataire satisfera à un certain niveau de qualité prédéfini, tout reposant sur des critères objectifs de mesure de performance pour les différents services. Concrètement, cet engagement permet de mettre en place des niveaux de service (délais d'intervention, garantie de service, ...) avec des éventuelles pénalités à la charge du prestataire en cas de manquement à son obligation. Il faudra donc que les deux parties soient tout particulièrement vigilantes à l'insertion d'une telle clause. C'est en effet souvent une des principales causes de mise en jeu de la responsabilité du prestataire.

La question de la durée du contrat. De préférence, celle-ci doit être courte afin de permettre au client de pouvoir renégocier le contrat. Le but est ainsi de pouvoir tirer avantage des prix pratiqués par la concurrence. Rappelons que les parties ont la possibilité de **résilier** le contrat à tout moment en respectant la procédure classique et en respectant un délai de préavis lorsqu'une des parties a manqué à une de ses obligations.

La question de la loi applicable et celle du **tribunal compétent** devra également être regardée par le client. Les contrats cloud peuvent revêtir un caractère international, il est à ce titre important d'intégrer une clause concernant ce point précis.

L'analyse de risque et la négociation contractuelle sont impératives et requièrent l'intervention du juriste dès la phase de conception du projet cloud. Il est indispensable de définir et circonscrire le périmètre de responsabilité de chacun. Outre la négociation du contrat, l'entreprise devra également sensibiliser son personnel aux risques liés au cloud.

III - Cloud et assurances

1. Impacts et limites de l'usage du cloud sur les assurances

Aujourd'hui, il est compliqué d'avoir une vision claire du paysage assurance et de sa réponse sur les conséquences de l'utilisation du cloud sur les programmes d'assurance.

Les risques immatériels et les nouveaux environnements techniques du cloud computing n'obéissent qu'imparfaitement à la traditionnelle distinction entre l'assurance de Dommages et l'assurance en Responsabilité Civile. Les risques induits par le cloud et plus généralement par la protection des actifs intangibles d'une société (c'est-à-dire son patrimoine immatériel) doivent faire appel à ces deux notions :

Le risque de dommage propre : les dommages aux données traitées par le cloud SaaS et stockées dans le cloud restent à la charge du responsable du traitement des données.

Le risque de responsabilité subi par des tiers : le fournisseur de cloud SaaS et l'opérateur de cloud engagent leur responsabilité de services (et non pas de produit logiciel) pour autant que leur faute soit démontrée et le préjudice quantifié et dans la limite des niveaux de service (SLA).

L'appréciation du préjudice comporte des dimensions très difficiles à quantifier (perte de confiance, perte d'image, perte d'intégrité ou de valeur probante d'une donnée) qui rend parfois difficilement applicable le principe indemnitaire. La transposition dans la réponse assurance est souvent très compliquée et reste à inventer. Et reste à inventer !

Les coûts suivants peuvent être pris en charge par les contrats d'assurance sur les atteintes aux actifs immatériels de l'entreprise :

Frais de reconstitution de données, qu'on retrouve souvent dans des contrats de type « tout risque informatique », ou fraude. Dans les frais de reconstitution, il faudrait considérer les **frais de réversibilité** qui correspondent aux coûts engendrés par la réinternalisation par l'entreprise ou la reprise par un tiers des services hébergés sur le cloud. S'ils ne sont pas pris en charge dans le SLA, ces coûts doivent être prévus dans le contrat d'assurance. Les définitions classiques de frais de reconstitution n'intègrent pas ces conséquences.

Frais supplémentaires d'exploitation, qui sont les frais nécessaires à la remise à niveau du service tel qu'il existait antérieurement au sinistre. L'évènement déclencheur de cette garantie diffère d'un contrat à l'autre : atteinte aux données, atteinte aux systèmes de l'assuré, dommage matériel, dommage accidentel et non malveillant….

Une prise en charge des frais de notification doit être envisagée. L'entreprise se doit d'être proactive, notamment face aux nombreuses possibilités d'investigation des autorités de régulation (AMF, ACP, CNIL…). L'entreprise peut être amenée à engager des frais auxquels il n'y a pas toujours de réponse assurantielle correspondante. Et, en cas d'enquête ou de sanction du régulateur, les

conséquences financières supportées par la société ne sont pas toujours prévues par les contrats d'assurance classiques.

2. Qu'évoquer avec son assureur ?

Le Risk Manager a pour vocation de recenser les différents risques qui pourraient mettre en péril l'atteinte des objectifs de son organisation.

Une fois cette analyse effectuée, son rôle est de proposer des solutions de gestion de risques adaptées, notamment au niveau d'appétence au risque de son organisation. Ex : actions de prévention à renforcer pour éviter la survenance du risque, action de transfert aux assurances, ...

À ce titre, il possède une méthodologie lui permettant d'analyser globalement l'ensemble des impacts engendrés par la survenance d'un risque majeur sur l'entreprise, tel **le cyberrisk par exemple** : impacts opérationnels, en France et/ou sur les différentes filiales à l'étranger ; impacts financiers ; impacts sur les processus transverses : achats, juridique, RH ; impacts sur l'organisation : PCA, gestion de crise, communication de crise ...

C'est pourquoi son apport est essentiel à l'analyse des risques SI et complète utilement celle effectuée par les experts informatiques de l'organisation, le plus souvent le RSSI et/ou le DSI.

Ce travail en commun, concernant le cloud computing par exemple, va lui permettre tout d'abord de bien comprendre la nature de l'exposition, les mécanismes de survenance. Cette phase est importante car elle doit lui permettre d'avoir une première vue sur le niveau de protection de son organisation (physique et contractuelle) et de vérifier que ce risque est bien couvert par ses assurances, notamment pour le risque résiduel. Il pourra alors faire le point sur les couvertures assurance en vigueur et le cas échéant les adapter/compléter pour optimiser le transfert (par exemple en cas de survenance d'un nouveau produit d'assurances plus adapté à sa situation sur le marché) ou de faire en sorte de se poser les bonnes questions, de faire ressortir les problématiques, si ces couvertures sont insuffisantes ou inadaptées…

De plus, en recensant les modalités de prévention/protection techniques et contractuelles mises en place, le Risk Manager sera aussi à même de proposer aux autres partenaires internes avec lesquels il est régulièrement en contact (achats, juristes, services généraux, RH,…), des évolutions utiles pour l'organisation, en terme de processus interne par exemple ou d'évolutions de plans d'actions. En fonction de ses différentes missions, il pourra ainsi suggérer d'adapter ou réadapter le Plan de Continuité d'Activité

Le Risk Manager, rompu à ces analyses, est un apporteur de méthode ainsi qu'un aiguillon au questionnement. Cette analyse commune, et indispensable avec les experts informatiques internes, peut même devenir une opportunité pour réaliser une analyse touchant aux dimensions transverses du SI.

Enfin, si cette mission lui est confiée, le Risk Manager complétera utilement la cartographie des risques de son organisation et suivra son évolution et les plans d'actions associés.

Avant de contacter son assureur il est indispensable de réaliser une analyse de risque et d'en dresser une cartographie. Pour avoir une bonne correspondance assurantielle, il faut connaître l'ensemble des risques et les conséquences financières associées.

L'utilisation de solution cloud est une évolution du risque lié aux systèmes d'information plutôt qu'une aggravation en tant que tel. C'est cette évolution qui doit être appréhendée afin de pouvoir en transférer les conséquences vers l'assurance. Une fois que les risques associés sont identifiés, il convient alors d'analyser la portée des garanties existantes avant de rechercher les solutions d'amélioration des programmes ou de nouvel achat de garanties

Souvent un constat s'impose, les contrats de Dommage ou de Responsabilité Civile présentent des limites à l'application dans le contexte du cloud.

Les contrats Dommage sont limités dans l'appréhension de notions comme la « donnée », par exemple, qui ne peut être considérée comme un bien ou une chose assurée au sens du contrat. Cela soulève des questions dont les réponses restent à définir. Par exemple, en l'absence de dommages matériels, est-ce qu'une garantie peut être délivrée sur les contrats de type Dommage en cas d'atteinte aux données ?

Pour les contrats en Responsabilité Civile, les atteintes de type virus ou cyber- attaque sont souvent exclues. Des contrats dits « Cyber » apparaissent depuis deux ou trois ans, mais l'offre n'est ni homogène, ni mature. La notion de « système informatique » de l'assuré pose une vraie difficulté : avec le recours au cloud où commencent ces systèmes, où s'arrêtent-ils ? Si l'entreprise n'a ni la maîtrise du cloud, ni de la localisation des serveurs de ses prestataires, il est fort à parier que le contrat se limitera à une définition classique de la notion de système d'information. Afin de répondre aux exigences des assureurs, il s'agirait pour l'entreprise de dresser la liste de tous les info-gérants, fournisseurs de services et sous-traitants ce qui est éminemment compliqué au vu des éléments présentés précédemment.

Ces deux phases d'analyse de risque et de sa cartographie, et d'analyse des contrats sont impératives pour trouver une solution assurantielle complémentaire. La solution assurantielle actuelle est imparfaite, et la solution de transfert doit être bâtie, au cas par cas.

Une autre solution pourrait consister en la mise en place d'une solution captivée de type « pertes financières tout causes ». Quoi qu'il en soit, les assureurs ont besoin que l'entreprise fournisse des données pour délivrer des solutions performantes. C'est donc aux entreprises de collecter les données sur les risques, les pertes, la quantification des pertes. C'est à force d'expérience que les entreprises auront la meilleure solution de transfert.

Quelques conseils dans le cadre de la négociation des contrats de service cloud :

- **Imposer des clauses de responsabilité et non d'irresponsabilité : miser sur la concurrence**

Souvent les clauses imposées par les acteurs vident l'obligation principale de sa substance.

Lorsque leur objet n'est pas trop limitatif, c'est le montant de l'indemnité qui est manifestement insuffisant au regard des conséquences que peuvent subir les sociétés.

Ce point est majeur car l'assureur pourrait interpréter certaines clauses comme des renonciations à recours que l'assureur peut valablement opposer à l'assuré pour refuser une prise en charge, au motif que la clause le prive lui-même de tout recours contre l'auteur du dommage ou son assureur.

- **Exiger de vrais contrats d'assurance**

Il convient en outre d'exiger la preuve de la souscription d'un contrat d'assurance de responsabilité avec des capitaux d'assurance en rapport avec les risques encourus. **Nous constatons trop souvent que ce point n'est pas traité dans les SLA. Quand l'assurance est exigée, les entreprises oublient souvent de vérifier la nature et le montant des garanties souscrites par les prestataires en demandant que soit fournie une attestation d'assurance, demande qu'il convient de renouveler tout au long de l'exécution de la prestation.**

IV - Les actions pour le Risk Manager

Ce Cahier technique est adressé aux Risk Managers, qui, selon l'organisation dans laquelle ils évoluent, assument tout ou partie du Risk Management.

En 2013, l'AMRAE a créé un référentiel métier du Risk Manager, posant un cadre de compréhension des activités, des tâches et des compétences portées par le Risk Manager[2]. Les missions suivantes ont été identifiées comme faisant partie de son périmètre :

- **Définition** des missions et de la structure du dispositif
- **Appréciation** du risque (identification, analyse, évaluation du risque)
- **Maitrise** des risques (au niveau acceptable en fonction des critères de risques retenus)
- **Diffusion** de la culture du risque
- **Financement** des risques en accord avec la politique de management des risques
- **Gestion** des événements non assurés/ non assurables
- **Gestion** des sinistres
- **Gestion** de crise
- **Pilotage**, reporting

Le Risk Manager peut donc, du fait de ces missions, avoir à appréhender les risques liés au cloud computing. Voici quelques clés pour appréhender avec succès les problématiques et enjeux liés à un projet cloud.

1. Qu'évoquer avec les métiers ?

D'une part, il s'agit de bien comprendre la demande, le contexte et son origine. Il est important de comprendre la position des acteurs internes et ce qu'ils attendent du cloud. Le Risk Manager (RM) doit être capable d'identifier les acteurs qui soutiennent le projet, ceux qui sont neutres et ceux qui sont en opposition.

D'autre part, le RM doit s'assurer que les métiers comprennent les limites et les contraintes du système au-delà du discours commercial des fournisseurs et des effets de mode qui mettent actuellement le cloud sous les feux de la rampe.

Il existe différents thèmes sur lesquels sensibiliser les métiers :

[2] Le référentiel métier est disponible en libre téléchargement sur le site de l'AMRAE (anglais et français) à cette adresse : http://www.amrae.fr/risk-manager-referentiel-metier

- **La dispersion géographique des données** : les données peuvent être hébergées sur des systèmes à l'étranger, sans même que l'entreprise en soit avertie.
- **Les juridictions différentes**, selon l'hébergement des données, le fournisseur...
- **La notion de données personnelles** : trop souvent, les métiers pensent que le fournisseur est responsable en cas d'incident. Ce n'est pas nécessairement le cas : l'entreprise reste en général responsable en cas de perte, vol ou corruption des données – on parle ici de responsabilité au sens juridique, mais c'est encore plus vrai en termes d'image : par exemple pour un client particulier en e-commerce, c'est le cybermarchand qu'il tient naturellement pour responsable de la bonne gestion de ses données personnelles, et non l'éventuel fournisseur/hébergeur du cybermarchand.
- **Les problématiques de confidentialité des données** : certaines données, comme par exemple un plan stratégique ou des données relatives à des incidents critiques, sont sensibles. Leur externalisation est donc une prise de risque que les métiers doivent connaître et apprécier en particulier dans des contrats de concurrence internationale.
- **La disponibilité des données** : le RM doit insister sur le fait que la disponibilité ininterrompue des données n'existe pas. Deux raisons peuvent expliquer ceci. La première est que même les géants informatiques connaissent des pannes, l'entreprise n'est pas à l'abri d'une interruption de service due à un incident chez le fournisseur. La seconde est que l'entreprise doit très souvent avoir accès à internet pour utiliser le cloud. La hantise de toute DSI est le « coup de pelleteuse » qui coupe un câble ou une fibre optique, privant ainsi l'entreprise de l'accès à Internet.
- **Il faut s'assurer que les exigences de continuité de service du métier sont raisonnablement couvertes** par les engagements contractuels du fournisseur. Le RM peut être amené à faire mûrir ces exigences : les métiers répondent souvent avoir besoin d'une disponibilité parfaite de l'application ou du service, ce qui est rarement le cas en réalité. Ceci permettra par exemple de définir un délai maximal d'interruption admissible réaliste par rapport aux enjeux et aux ressources que l'entreprise peut y consacrer. Le coût croît en général très fortement avec la disponibilité exigée (un système avec une disponibilité garantie de 99,9% coûte classiquement beaucoup plus cher qu'un système avec une disponibilité garantie de 99%).
- **Se préparer à une éventuelle interruption de service** : inévitablement, le service connaîtra une panne un jour ou l'autre. L'entreprise doit s'y préparer. Exemple : identifier les activités sensibles, construire leur plan de continuité, tester et gérer les crises…

2. Qu'évoquer avec la DSI ?

Avant tout, **il est nécessaire que le RM comprenne quel est le niveau d'implication de la DSI et du Responsable de la Sécurité des Systèmes d'Information (RSSI) dans ces contrats.**

Le cloud permet parfois aux opérationnels d'outrepasser les dispositifs de contrôle interne. En théorie, aucun directeur marketing, par exemple, ne peut acheter seul puis installer dans les locaux de l'entreprise un système informatique classique sans travailler avec les achats, la DSI, le juridique…

En revanche, acheter un service cloud peut être fait de manière très simple, sans que l'informatique interne ni les achats ne soient au courant. Parfois, le demandeur métier ne sait même pas que le service qu'il achète utilise des technologies cloud (ex. classique en B-to-C : opération promotionnelle commandée à une agence, opération incluant un ou plusieurs « mini-sites » web, l'agence gère avant tout la partie créative et délègue l'exploitation à différents fournisseurs et hébergeurs qui peuvent avoir recours à des technologies cloud sans que le client final en ait vraiment conscience).

Comme évoqué précédemment, l'Informatique Interne peut être rebutée par le cloud, qui suscite parfois des inquiétudes organisationnelles. La DSI évolue de manière fondamentale, d'un rôle de concepteur de systèmes vers un rôle de prestataire de service pour les métiers et/ou de gestionnaire de contrats d'externalisation. Ceci peut soulever des préoccupations RH de la part des collaborateurs.

La notion d'implication de la DSI est très importante. **Dès l'origine des initiatives cloud, il est recommandé de mettre en place une Task Force** composée de juristes, des demandeurs, des achats, de la DSI, du RSSI et du Risk Manager. Si le RM ne s'occupe pas des assurances alors le responsable des assurances doit aussi faire partie de la Task Force.

L'entreprise, par ses hommes de l'art, doit poser un ensemble de questions aux fournisseurs potentiels avant toute contractualisation :

- Comment le fournisseur gère-t-il les vulnérabilités signalées sur les systèmes qu'il emploie ? Y-a-t-il une procédure de notification des brèches et incidents de sécurité ? Possède-t-il une procédure d'alerte et d'escalade ? Cette question est fondamentale pour le RSSI, a fortiori s'il a la gestion de crise dans son périmètre : les dispositifs de gestion de crise de l'entreprise et de son fournisseur de services cloud doivent être connectés de manière opérationnelle (exemple de détail pratique : langue de communication d'urgence avec un fournisseur transnational). Le fournisseur doit être obligé de notifier l'entreprise dans un délai court en cas de problème.

- Quelles sont les pratiques de sécurité du fournisseur? Est-il dans un processus d'amélioration continue, c'est à dire une démarche très structurée du type ISO 27001 ou ISO 9001 ? Est-il plutôt dans une approche moins mature de « cases à cocher » (qui consiste à lister des besoins de sécurité et vérifier leur couverture, par exemple : antivirus oui / non) ?

- Quel type de chiffrement des données le fournisseur utilise-t-il ? Plus le chiffrement est sophistiqué, plus l'entreprise se protège des problèmes de confidentialité. Cependant, le revers de la médaille est qu'en cas de problème (par exemple une défaillance d'un disque dur), une donnée chiffrée est beaucoup plus difficile (voire impossible) à récupérer qu'une donnée non chiffrée.

- Y-a-t-il un interlocuteur "sécurité" prévu ? Des échanges réguliers sur ces sujets peuvent-ils être prévus (dans la revue annuelle du contrat, par exemple) ? Est-ce que le fournisseur « aime » parler sécurité, ou est-il réticent, fuyant ou trop rassurant sur le sujet (« il n'y a jamais de problèmes ») ?

L'entreprise doit avoir une possibilité concrète de sortir du contrat : les clauses de sortie existent en général, mais doivent pouvoir être appliquées en pratique, ce qui est moins systématique. Cette sortie « physique » doit pouvoir se faire sans mettre en péril l'activité de l'entreprise et la qualité de

service interne et externe. Avec une réelle possibilité de sortie, l'avantage pour l'entreprise est qu'elle se retrouve davantage en position de force par rapport à son fournisseur. Le fournisseur sait alors qu'il n'est pas en « terrain conquis » et sera en général plus réceptif aux demandes du client, ce qui favorisera une relation équilibrée – bonne illustration de l'adage romain « si vis pacem, para bellum ».

Le Risk Manager peut avoir à se pencher sur les problématiques liées à la continuité d'exploitation dans l'entreprise. Il s'agit là encore de se poser la question de l'implication de la DSI. Par exemple, historiquement, la connexion Internet n'est pas considérée comme faisant partie des services les plus critiques, par rapport au réseau interne par exemple. Or, dans le contexte du cloud, elle est vitale. Le RM doit donc poser les questions suivantes :

- L'accès Internet est-il redondé ?
- Combien de fournisseurs différents y-a-t-il ?
- Selon le nombre et la qualité des fournisseurs, faut-il contracter avec un nouveau prestataire ?
- Est-ce que les différentes sorties vers les fournisseurs sont situées au même endroit sur la voie publique ? Si oui, il y une vulnérabilité liée au fait que le même incident (ex. « coup de pelleteuse ») peut couper tous les accès Internet vers les différents fournisseurs ; « bonne pratique » classique : deux fournisseurs différents, avec des raccordements aux réseaux externes situés à l'opposé par rapport au terrain occupé par l'établissement)

V - Conclusion

Le cloud computing est une évolution fondamentale des systèmes d'informations, qui modifie le quotidien de ses utilisateurs, DSI et métiers. Aux promesses du cloud – souplesse, réactivité, économies – sont associés des risques relatifs à la confidentialité des données, la maîtrise et la cohérence du système d'information et la cybercriminalité. En effet, si le cloud présente un intérêt pour les entreprises, il attire également les cybercriminels et les États, qui l'utilisent souvent à des fins d'intelligence économique. Ces risques sont cependant à relativiser : **les entreprises sont confrontés à une évolution de la nature des risques plus qu'à l'apparition de nouveaux risques.**

Le cloud computing entraîne enfin des évolutions sur le plan juridique et assurantiel. La **relation client / fournisseur est transformée** du fait de la structure du marché du cloud computing et des enjeux de contrôle, de sécurité et de traçabilité des données. La contractualisation, plus que jamais, s'avère une étape clé de la relation.

Il implique une **évolution de la relation avec l'assureur** dans un marché encore en maturation.

Dans ce contexte, le Risk Manager doit avant tout faire reconnaître qu'il a voix au chapitre dans les projets de cloud, au même titre et aux côtés du RSSI.

Le Risk Manager doit comprendre en profondeur le projet et réaliser une analyse de risques en se posant les bonnes questions : que veut faire l'entreprise ? Quels sont les acteurs de ce projet ? Quels sont les intérêts des acteurs ? Quel est le niveau de maturité collectif (métier/DSI) sur ces sujets ?

Le Risk Manager doit traiter les impacts du projet sur son domaine d'activité, ce qui inclut les assurances bien sûr, mais également les divers travaux sur le risque effectués auparavant : analyses de vulnérabilités, analyses de risques et cartographie. Ces travaux doivent être revisités car un certain nombre d'hypothèses implicites ou explicites reposent sur un modèle « traditionnel », c'est-à-dire un SI interne, opéré dans les locaux de l'entreprise, bien protégé physiquement, sur lequel opèrent uniquement des salariés de l'entreprise. Il s'agira également de bien comprendre l'impact métier, qui est souvent supérieur à celui perçu au premier abord. Enfin, si le RM s'occupe des sujets de continuité d'activité et de gestion de crise, des travaux significatifs sont à prévoir pour mettre à jour et adapter ces dispositifs au cloud – et si ces domaines ne sont pas dans son périmètre, il doit a minima s'assurer que les personnes en charge de ces sujets sont conscientes des impacts.

- - -

Cloud Computing : les questions clés que doivent se poser les Risk Managers
25 pages

Décembre 2013

Bureau Permanent AMRAE -Tél: 01.42.89.33.16. - amrae@amrae.fr

LES CAHIERS TECHNIQUES DE l'AMRAE

Cette Collection regroupe plus d'une dizaine de publications qui sont le produit des échanges, réflexions et travaux des Commissions et Groupes Thématiques de l'AMRAE.

Les Cahiers Techniques sont conçus et rédigés par des Membres de l'AMRAE, afin de partager leur expertise et expérience, avec un objectif pragmatique et concret.

Déjà parus :

- Analyse et présentation des travaux de l'AMF relatifs à la gestion des risques et au comité d'audit
- Etat des lieux en Responsabilité Civile : les exclusions
- Flottes automobiles - l'auto-assurance : opportunité ou risque pour votre entreprise
- Les managers opérationnels face à leurs responsabilités. Prévention et protection
- L'infogérance : externalisation de services informatiques et gestion des risques
- Panorama SIGR 2013
- RMIS Panorama 5th ed.
- Paroles d'experts : Actualité en matière de transport de marchandises
- Expert opinions : Recent developments in goods transport
- Programmes d'assurances internationaux
- Insurance International Programmes
- REX sur un contentieux anglo-saxon
- RM et RH : Pourquoi et comment travailler ensemble ?

Les Cahiers Techniques sont téléchargeables gratuitement au format PDF pour les Membres AMRAE sur le Site AMRAE.

Les Cahiers Techniques sont également disponibles à la vente (exemplaires papier).

Librairie en ligne et accès PDF (pour les membres AMRAE)
www.amrae.fr/Publications

AMRAE | 80 boulevard Haussmann 75008 Paris | www.amrae.fr

Tel. +33 (1) 42 89 33 16 | amrae@amrae.fr