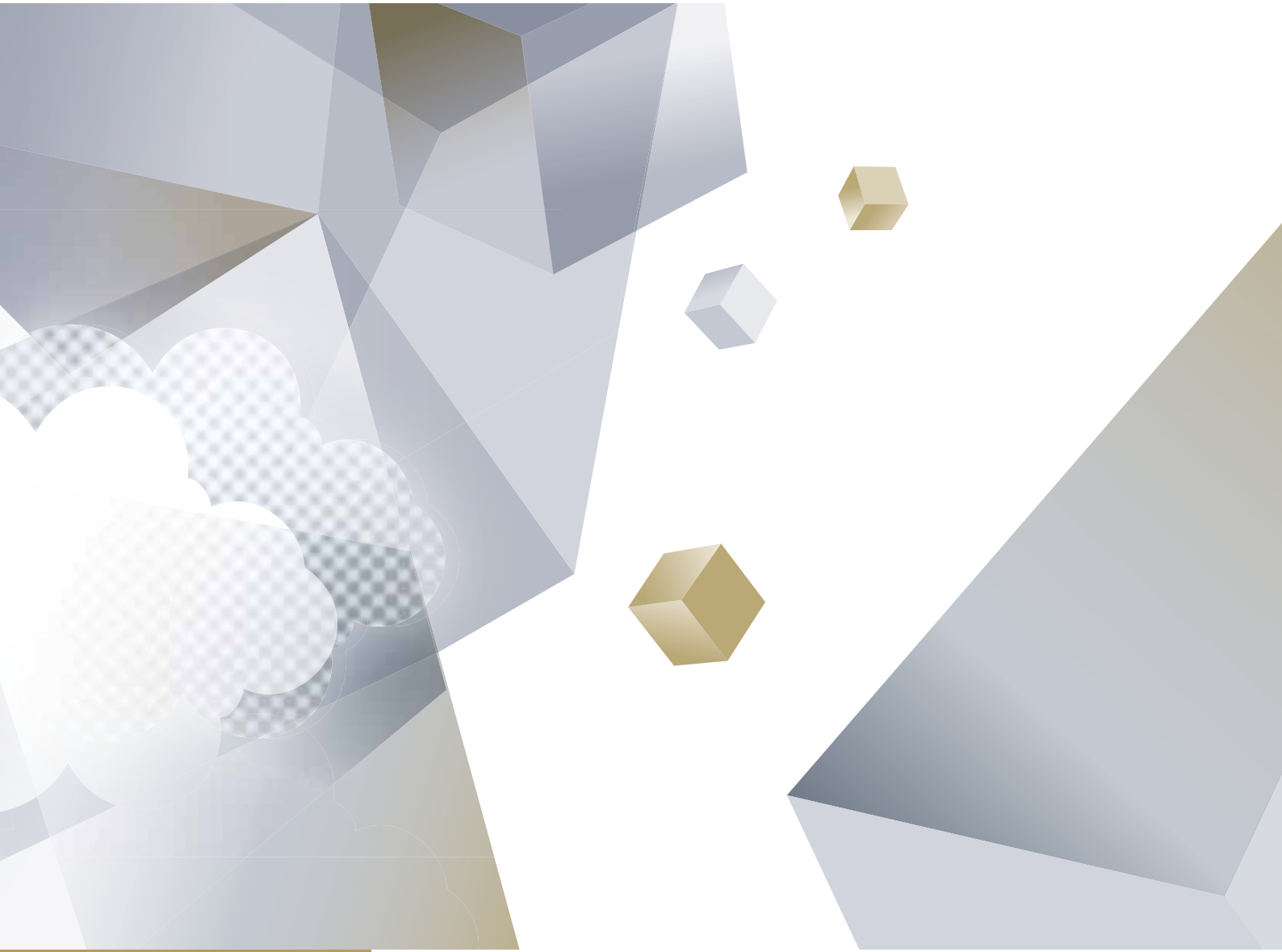
Syntec NUMERIQUE
DES ENTREPRISES QUI CHANGENT LE MONDE

# CLOUD COMPUTING
## NOUVEAUX MODÈLES !

Modèles économiques, contrats, relations clients-fournisseurs, organisation de la DSI : tout ce qui change avec le Cloud



**LIVRE BLANC** | MARS 2012

En partenariat avec CRiP Infrastructure & Production — AFSCM

## Avis aux lecteurs

Comme pour les deux précédents volumes («Cloud Computing : ce qu'il faut savoir» et «La sécurité du Cloud Computing»), ce livre blanc est un travail original de ses contributeurs. Il évite d'emprunter aux publications existantes, qu'elles soient internationales ou françaises, institutionnelles ou privées. Il en est de même des nombreux schémas, illustrations et tableaux de synthèse réalisés à l'occasion de cette publication.

Le présent livre blanc «Cloud Computing : Nouveaux modèles!» – rédigé de septembre à décembre 2011 – soulève les questions clés que chacun s'est posé en cette année de rédaction. Les réponses proposées ont cours à cette date, sans trop anticiper les évolutions – toujours fulgurantes – que l'on est en droit d'attendre de ce domaine.

Nous apprenons tous l'informatique dans le nuage en avançant... avec réalisme, modestie et enthousiasme !

Ce livre blanc n'est pas le fait d'une société privée mais d'un groupe de travail constitué de fournisseurs, de grands clients et des représentants du chapitre français du référentiel eSCM. Voilà pourquoi les rédacteurs se sont livrés à un effort permanent visant à regarder les problématiques sur «360°», côté client, côté fournisseurs et prenant en compte – lorsqu'ils diffèrent – les points de vue Cloud privé/Cloud public.

**La rédaction**

# ÉDITO

Vous tenez entre vos mains le troisième livre blanc que Syntec Numérique, et plus précisément le comité Infrastructures, a réalisé en quelques mois sur le thème du Cloud Computing*.

Original et tout à fait exclusif, cet ouvrage n'est pas le seul fruit des membres de Syntec Numérique. C'est aussi le travail d'une collaboration inédite avec les représentants du CRIP (Club des responsables d'infrastructures et de production informatique) et ceux de l'Ae-SCM, association pour la promotion des bonnes pratiques de sourcing.

Personne ne peut contester l'ampleur du phénomène du Cloud : d'abord « concept », suivi d'un « alignement technologique » des grands acteurs, puis « offre marketing », nous voici parvenus – à l'aube de cette année 2012 – au moment charnière où la demande des grandes, des moyennes comme des toutes petites entreprises, se concrétise.

Là, se posent d'autres questions, d'importance. Celles tenant de la remise en cause par le Cloud Computing des modèles :

- Pour les entreprises clientes : la contractualisation, le rôle et le fonctionnement de la DSI, les évolutions des compétences internes, la remise en cause des aspects économiques (Opex/Capex, ROI, valeurs intangibles...), les modèles d'architectures hybrides (coopération Cloud avec le SI existant), les standards, normes et autres problématiques de réversibilité...

- Pour les entreprises de l'offre : les modèles économiques, le partage de la valeur, les nouveaux partenariats, la contractualisation et les engagements (SLAs), les problématiques d'interopérabilité des Clouds...

Voilà donc les thématiques, et le pourquoi, de ce livre blanc « Cloud Computing : Nouveaux modèles ! »

Donner des éclairages sur tous ces points – sans forcément chercher à y répondre de manière péremptoire et définitive, car ce domaine est encore tout neuf – c'est amener à réflexion, à la recherche de solutions et à terme, à la confiance entre les parties concernées.

Fruit d'un « dialogue constructif » auquel les uns et les autres se sont livrés, côté fournisseurs comme côté clients et association, le ton du livre est « autre » et les sujets élargis, traités sur 360°. Nous souhaitons qu'il vous en soit que plus utile.

**Excellente lecture !**

**Philippe Hedde,**
**Président du Comité Infrastructures**
**Syntec Numérique.**

* Les deux premiers livres blancs publiés début et fin 2010 par Syntec Numérique traitaient les concepts, atouts et limites du Cloud Computing ainsi que ses problématiques sécuritaires spécifiques (ouvrages en libre téléchargement sur le site www.syntec-numerique.fr).

# SOMMAIRE

# 1. INTRODUCTION

## 1.1. Sur le Cloud, en général

Le terme « Cloud » désigne aujourd'hui de manière générale un nouveau modèle à la fois de distribution et de consommation de l'informatique qui consiste à mettre à disposition via les réseaux de communication et à la demande (= « as a service »), un ensemble de « ressources » (puissance de calcul, stockage de données, applications, etc.) et de « services » (gestion, administration, etc.). Celles-ci seront mutualisées, dématérialisées, contractualisées, évolutives et en libre-service.

Les solutions cloud reposent principalement sur des technologies de virtualisation et d'automatisation. Trois caractéristiques clés du Cloud le différencient de l'informatique traditionnelle :

- Mutualisation et allocation dynamique de capacité (adaptation élastique aux variations de charge).
- Services à la place de produits technologiques avec mise à jour en continu et automatique.
- Self-service et paiement à l'usage (en fonction de ce que l'on consomme).

### 1.1.1. Typologie

Les machines, applications et données pourront être disséminées ou centralisées dans un, ou dans différents sites internes, chez des prestataires, dans un Data Center situé à l'autre bout de la planète ou sur une myriade de serveurs constituant un même « nuage » (cette dernière métaphore est utilisée depuis les années 90 pour représenter les réseaux et en particulier Internet).

**Les machines, applications et données** pourront être disséminées ou centralisées dans un, ou dans différents sites internes, chez des prestataires, dans un Data Center situé à l'autre bout de la planète ou sur une myriade de serveurs constituant un même « nuage ».

Le Cloud Computing, tel que défini par le NIST (*National Institute of Standards and Technology*), est constitué de différentes composantes – dont il est indifféremment l'une, les deux ou les trois combinées :

- **SaaS (Software as a Service)** : concerne la mise à disposition d'applications d'entreprise : CRM, outils collaboratifs, messagerie, Business Intelligence, ERP, etc. Le fournisseur offre une fonction opérationnelle et gère de façon transparente pour l'utilisateur l'ensemble des aspects techniques requérant des compétences informatiques. Le client garde la possibilité d'effectuer quelques paramétrages de l'application.

- **PaaS (Platform as a Service)** : concerne la mise à disposition de plates-formes de middleware, de développement, de test, d'exécution d'applications… Le fournisseur gère et contrôle l'infrastructure technique (réseau, serveurs, OS, stockage…). Le client garde la main sur le déploiement des applications, sur leurs paramétrages.

- **IaaS (Infrastructure as a Service)** : concerne la mise à disposition de ressources informatiques (puissance CPU, mémoire, stockage…). Le modèle IaaS permet au client de disposer de ressources

virtualisées et déportées. Celui-ci garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple).

### 1.1.2. Modèles de déploiement

Différents modèles de Cloud coexistent :

- **Cloud privé internalisé** : « nuage » interne à l'entreprise (l'entreprise étant propriétaire et gestionnaire des infrastructures) ou Cloud entièrement dédié à cette même entreprise, accessible via des réseaux sécurisés, opéré par les équipes internes.

- **Cloud privé externalisé** : plate-forme de Cloud Computing qui vise à fournir, de manière externalisée, les services et garanties équivalents à ceux offerts par un Cloud privé interne, tout en bénéficiant des avantages des services de gestion par un tiers. Il peut être accessible par Internet ou par un réseau privé.

- **Cloud public** : il est externe à l'entreprise, accessible via Internet ou un réseau privé, géré par un opérateur externe propriétaire des infrastructures, avec des ressources totalement partagées entre tous ses clients.

- **Cloud hybride** : il s'agit de la conjonction de deux ou plusieurs Clouds (public+privé) amenés à « coopérer », à partager entre eux applications et données.

### 1.1.3. Quels Clouds pour quelles applications ?

En mode IaaS, la généralisation de la virtualisation des serveurs permet de multiplier les projets de type cloud. Dans ce mode, les environnements le plus souvent sujets à évolution sont :

- La virtualisation des postes de travail
- Les environnements de Test & Développement (car ils ont des besoins assez imprévisibles de ressource à la demande et sont en recherche d'élasticité).

Historiquement, les grands projets informatiques (ERP, par exemple) – statiques une fois bâtis – avaient jusqu'à récemment peu besoin d'élasticité (sauf en phase de test), et étaient gérés en mode « silo », dans lequel l'infrastructure de calcul et de stockage est dédiée à l'usage exclusif de cette seule application. Avec la plus grande flexibilité des activités des entreprises et des administrations qui s'accélèrent depuis 2 ou 3 ans, cette position est amenée à évoluer. Jusqu'à peu, la vue était que plus l'application est verticale, spécifique, « critique », moins elle est éligible au Cloud. Cette vue est clairement en train de changer, avec le développement des Clouds internes dans les grandes entités utilisatrices d'une part, et le foisonnement d'offres verticales de services cloud d'autre part.

**En mode IaaS**, la généralisation de la virtualisation des serveurs permet de multiplier les projets de type Cloud.

Ainsi, le Cloud s'avère particulièrement pertinent pour les applications à géométrie variable (test/développement, applications Web et e-commerce, etc.) ou pénibles à gérer : les postes clients, la messagerie, outils collaboratifs, CRM, solutions de gestion des ordres de mission et des notes de frais.

Pour chaque application clé – et quelle qu'elle soit – on devra se poser des questions sur le type de service cloud le plus opportun (IaaS, PaaS, SaaS) et sur le type de déploiement souhaité (privé/privatif, public ou hybride). Pour répondre à ces questions, deux catégories de critères doivent entrer en ligne de compte : métiers (réglementaire, culturel…) pour le mode de déploiement ; techniques, pour définir le service.

**le Cloud s'avère particulièrement pertinent** pour les applications à géométrie variable (test/développement, applications Web et e-commerce, etc.) ou pénibles à gérer.

## 1.2. Les bonnes pratiques du référentiel eSCM

Le référentiel eSCM regroupe un ensemble de bonnes pratiques de sourcing IT. Il propose deux versions « miroir », l'une pour les clients, l'autre pour les fournisseurs. chaque partie peut tirer avantage de ce référentiel pour améliorer ses aptitudes en matière de :

- Gestion de la relation client-fournisseur
- Gestion des risques
- Pilotage de la performance
- Gestion de la connaissance et des ressources humaines
- Contractualisation, conception, déploiement et transfert du service
- Fourniture et réversibilité du service.

Les deux modèles – eSCM-CL pour les clients et eSCM-SP pour les fournisseurs – sont organisés autour du cycle de vie du sourcing. Les pratiques successives sont complétées par des bonnes pratiques transverses, ou permanentes, qui traitent de gouvernance/valeur, de l'aspect humain (compétences, relations, conduite du changement) et environnemental (risques, technologies, réglementations). La nature des pratiques diffère selon le point de vue considéré, client ou fournisseur. Par exemple, des pratiques stratégiques et d'analyse amont sont prévues pour le client, mais pas pour le fournisseur. D'autres pratiques sont symétriques (par exemple pour la négociation).

Dernier né des référentiels de bonnes pratiques, eSCM est conçu pour être très modulaire, adapté à tous types de sourcing, et compatible avec tous les référentiels existants, d'ITIL à COBIT, CMMI, Prince 2, ISO 9001 ou 20000. Dans le contexte évolutif, multiforme, complexe du Cloud Computing, eSCM peut aider à structurer l'approche, les décisions et le pilotage de services, tant côté fournisseur que client.

## 1.3. Du changement dans l'air...

Les technologies supportant le Cloud ouvrent donc la voie à des changements concrets, rapides et surtout très attendus par les DSI clientes, en ce qu'elles lèvent bien des contraintes et apportent d'essentiels bénéfices. Il y a donc du changement dans l'air...

**Du côté de l'offre,** les modèles de financement, d'investissement, de rémunération sont remis en cause ; la chaine de valeur et la distribution des rôles va évoluer, et des compétences nouvelles vont devoir émerger chez les différents actesurs.

**Du côté de la demande,** l'impact du Cloud sera plus profond encore. Ainsi, sont remis en cause les « modèles » appliqués jusque-là : économiques, contractuels, relationnels, organisationnels et méthodologiques. Dans les chapitres qui suivent, cet ouvrage entend en expliciter les changements.

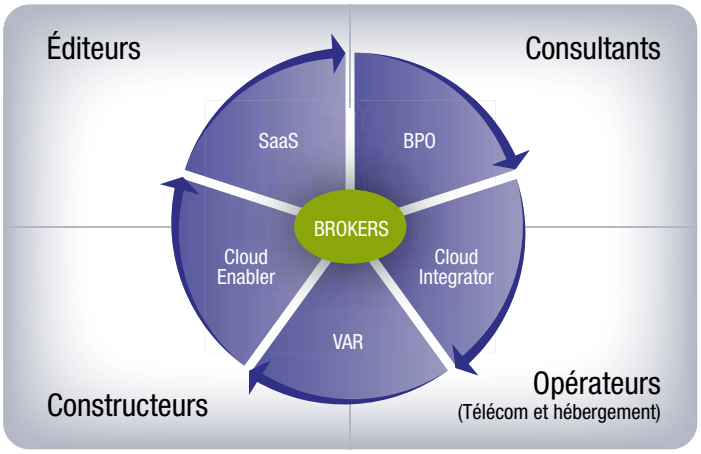
# 2. NOUVEAUX MODÈLES ÉCONOMIQUES DU CLOUD

## 2.1. Typologie des fournisseurs de Cloud

Côté fournisseurs, différents modèles coexistent :

- Un ou plusieurs « Cloud brokers » (courtiers, intermédiaires) ou « Cloud integrators » sont les interlocuteurs primaires du client, ils fédèrent ensuite un ensemble de « Cloud providers », eux-mêmes adossés à des partenaires et fournisseurs de technologie. Un « Cloud provider » de rang 1 peut être d'ailleurs le « broker », fédérant ensuite des fournisseurs de solutions Cloud de rang 2 ou N…
- Le « Cloud carrier » – qui fournit l'accès réseau nécessaire à l'obtention des services – est un acteur évidemment indispensable, distinct ou confondu avec le broker et le provider.
- Le « Cloud auditor » – qui assure les missions d'Audit (performances, sécurité, …)

Évolutions de la chaîne de valeur

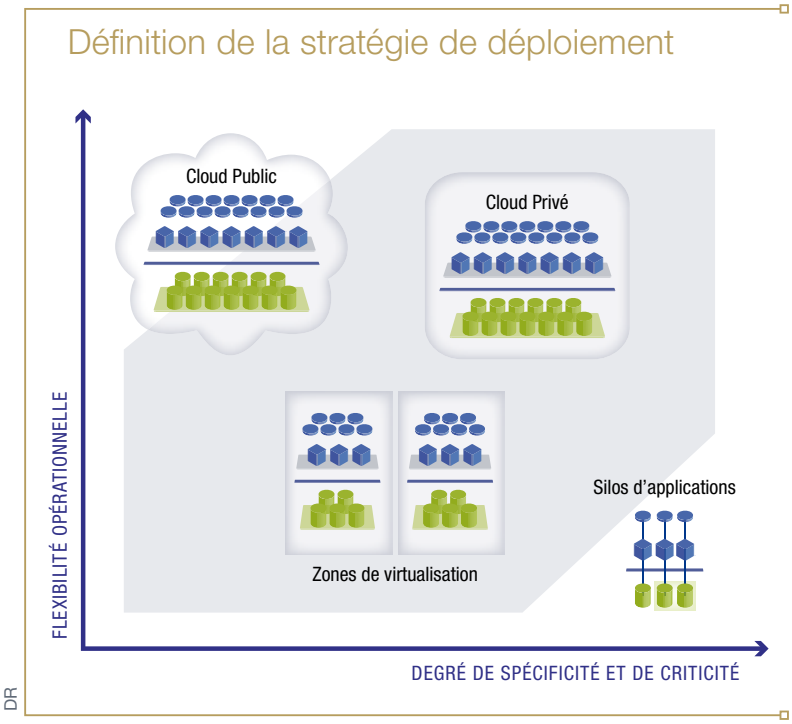



DR

Outre ces acteurs natifs, SSII, éditeurs, fabricants de matériel, acteurs majeurs des réseaux sont tous potentiellement des fournisseurs d'une offre de Cloud, ans parler des acteurs que l'on n'attendait pas : par exemple, l'état français se place dans un rôle multiple de client potentiel, de régulateur et désormais de fédérateur ou de promoteur d'acteurs nationaux, tels que le consortium Andromède.

### 2.1.1. éligibilité au Cloud

Le schéma ci-dessous illustre une méthode pour définir la stratégie de déploiement.
L'axe X représente le degré de spécificité et de criticité des applications : en général, lorsque celui-ci est élevé, les applications sont conservées




en interne. L'axe Y représente la flexibilité opérationnelle : un besoin de flexibilité important conduit à l'utilisation du Cloud dans la partie supérieure (par nature le Cloud fournit la flexibilité maximale).

- **Degré de spécificité et de criticité faible + flexibilité élevée :** les applications sont plutôt de bonnes candidates pour le Cloud public. Dans certains cas, certaines applications de « Software à la demande (SaaS) » peuvent être très stratégiques ou critiques (par exemple : la messagerie).

- **Degré de spécificité et de criticité faible + flexibilité faible :** les applications sont généralement de bonnes candidates pour la virtualisation. C'est d'ailleurs ce qui a fait le succès initial de la virtualisation des applications d'infrastructure.

- **Degré de spécificité et de criticité élevé + flexibilité élevée :** contexte favorable au Cloud privé pour la conservation en interne et bénéficier de tous les avantages du Cloud.

- **Degré de spécificité et de criticité élevé + flexibilité faible :** il s'agit de déterminer s'il faut conserver la situation telle qu'elle (en silo ?) ou passer à la virtualisation, mais le Cloud n'apparaît pas nécessaire sans la contrainte de flexibilité.

Il s'agit simplement de lignes directrices proposées par ce livre blanc dont l'application variera selon les impératifs de chaque organisation.

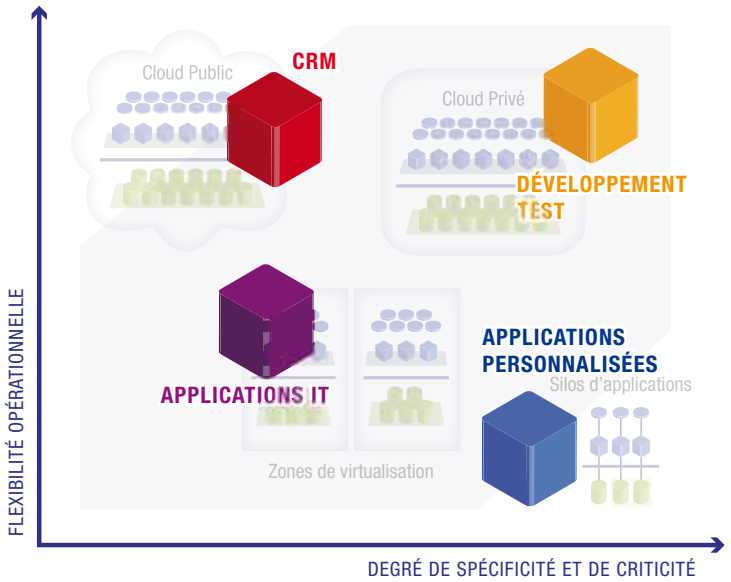
De plus, les besoins peuvent évoluer au fil du temps, nécessitant le passage à la virtualisation dans une première phase, et pouvant se révéler candidats au Cloud par la suite ou bien au passage direct en mode cloud.

**Le schéma suivant illustre ce modèle bidimensionnel.**

L'environnement CRM est souvent proposé par les fournisseurs de Cloud public. Les environnements Test/Développement sont souvent utilisés dans les Clouds privés. Les applications informatiques de différents degrés de spécificité et de criticité sont virtualisées des applications d'infrastructure et, de plus en plus, des applications vitales. Enfin se trouvent organisées en silos les applications :

- Personnalisées basées sur des architectures héritées et ayant une haute valeur stratégique.
- Ou plus récentes aux besoins spécifiques uniques.

Modèle bidimensionnel




**CLOUD PUBLIC**
- Applications secondaires
- Adaptation dynamique à la demande
- Libre-service et coût en fonction de l'utilisation
- Services clouds disponibles

**CLOUD PRIVÉ**
- Service essentiels définis
- Hautement dynamique
- Libre-service et analyses

**ZONES DE VIRTUALISATION**
- Consolidation des application informatiques essentielles
- Moyennement dynamique
- Aucun besoin libre-service

**SILOS D'APPLICATIONS**
- Besoins spécifiques aux applications en silos
- Matériel dédié et optimisé
- Environnement statique

DR

## 2.2. DSI/CTO : évaluer les apports et enjeux du Cloud par rapport aux modèles traditionnels

Le Cloud Computing permet à la DSI de devenir un prestataire qui propose à ses clients finaux des services informatiques à la demande. Ces services peuvent être achetés à un fournisseur tiers (Cloud externe ou public), ou provenir de la modernisation des propres ressources informatiques de l'organisation (Cloud interne) : il faut pour cela une infrastructure virtualisée et partagée, au provisionnement automatisé pour une allocation des ressources plus rapide, et des opérations

automatisées pour une gestion plus efficace. La bonne approche passe souvent par une combinaison de solutions de type Cloud internalisé et Cloud externalisé, privé et public.

Pour évaluer les apports de ce nouveau modèle, les DSI (avec les CTO – responsables des infrastructures et de la production informatique) doivent prendre en compte les postes suivants :

- **Le budget**
  - Infrastructure IT virtualisée générant des économies d'échelles
  - Retour sur investissement
  - Une approche TCO (comptabiliser tous les coûts, directs et indirects)
  - Capex (dépenses d'investissement en capital)
  - Opex (dépenses d'exploitation)
- **La maîtrise des coûts**
  - Prédictibilité (linéarité)
  - Refacturation aux métiers (meilleur contrôle de qui consomme quoi ?), cela nécessite des outils transverses pour un pilotage du SI dans son ensemble
  - Optimisation des ressources (bonne adéquation/alignement entre ce qui est engagé et le besoin réel)
- **La souplesse opérationnelle (flexibilité ou élasticité)**
  - Satisfaire de manière dynamique les besoins changeants ou nouveaux de l'entreprise
  - Disposer d'une meilleure réactivité ; réduction du temps nécessaire pour provisionner un système et activer une nouvelle application en passant de plusieurs semaines à quelques jours, ce qui permet :
    - Le développement et des tests d'applications accélérés
    - L'amélioration de la qualité et des délais de mise sur le marché
    - Un impact considérable sur l'aptitude de l'entreprise à innover
- **L'évolutivité**
  - En masquant la complexité, elle semble « transparente »
  - Elle paraît quasi-infinie
- **L'amélioration de l'efficacité**
  - Standardisation,
  - Meilleure affectation et utilisation des ressources (centralisation)
  - Simplification et automatisation des processus de provisionnement
  - Efficacité opérationnelle globale par l'automatisation de tous les aspects de la gestion informatique.

Alors... Cloud privé, public ou privé externalisé ? Les DSI étudient systématiquement les différentes approches :

- **En interne (derrière le firewall de la société) :** il apporte une meilleure sécurité et un certain contrôle mais... il faut maintenir et/ou développer les compétences.
- **En externe (sur Internet, via VPN ou connexion sécurisée) :** il suppose un couplage avec le fournisseur de services (contrat), la remise en cause des équipes en place et paraît plus simple (car ne reste dans l'entreprise cliente qu'éventuellement le pilotage).

*In fine*, l'approche retenue est souvent hybride.

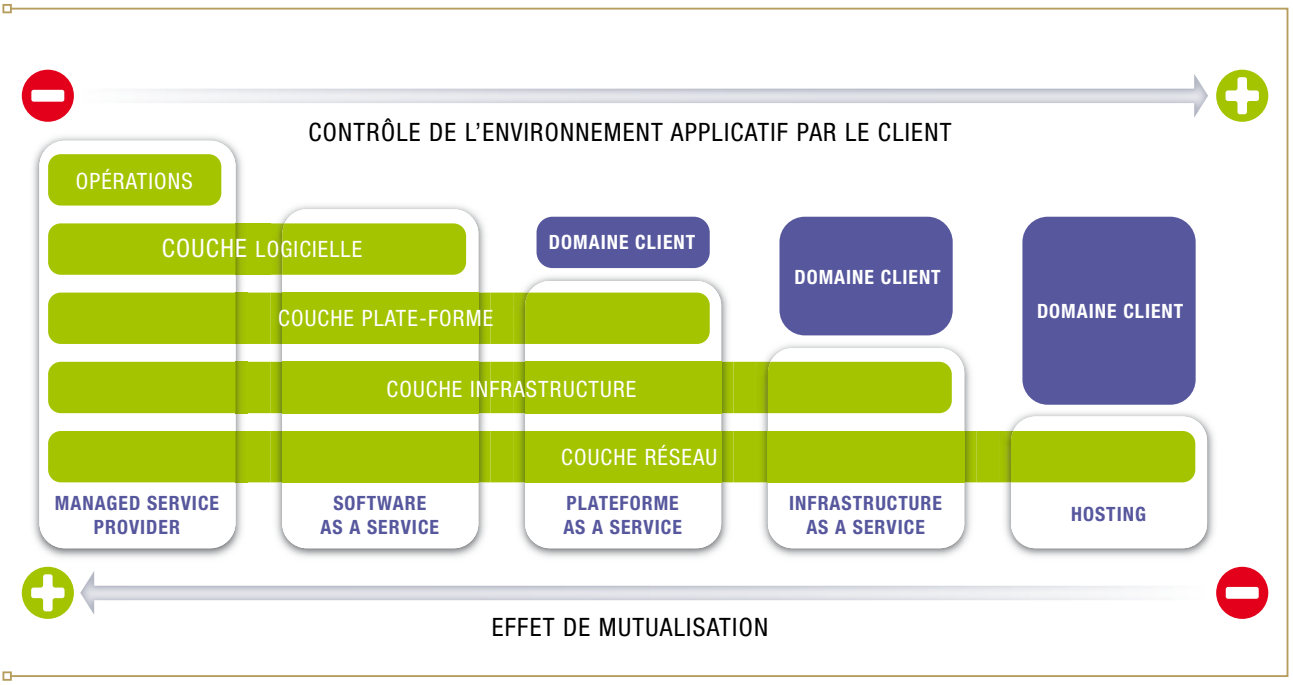
## La réduction des coûts, principal avantage attendu du Cloud

**L'enquête menée début 2011 par le CRIP auprès de ses membres montre que les responsables d'infrastructure et de production se préparent activement au Cloud Computing. En effet, 20 % des répondants avaient déjà entamé une démarche de mise en place d'un Cloud interne, principalement du type plate-forme IaaS (Infrastructure-as-a-Service) sous la forme d'un Data Center virtualisé et plus de 40 % des répondants envisageaient de se lancer dans un projet de Cloud interne dans les douze mois à venir. Ajoutons que près de 30 % des répondants envisageaient de lancer un projet de Cloud externe dans les douze mois. La réduction des coûts constituait pour 75 % membres du CRIP interrogés en 2010 l'attente principale vis-à-vis des services cloud.**

## 2.3. Des offres granulaires, à adapter aux opportunités

Bien que l'externalisation des applications informatiques existe depuis fort longtemps («infogérance»), le Cloud Computing vient souffler un vent nouveau sur cette discipline : il permet au DSI de disposer d'une granularité et d'une progressivité sans précédent en terme d'externalisation.

Hier, les offres d'externalisation de système d'information «métier» se cantonnaient souvent au «tout ou rien», à savoir l'infogérance complète (Managed Service Provider) ou l'hébergement «nu» ou presque. Aujourd'hui, les offres «cloud» permettent au DSI d'accéder à une toute nouvelle finesse de choix dans le niveau d'externalisation de son SI métier. En fonction du niveau de contrôle et/ou de personnalisation que la DSI veut garder sur son applicatif (et de la maturité de ses développements internes), elle optera pour du SaaS, du PaaS ou du IaaS. En découleront des économies substantielles, liées à un effet de mutualisation réalisé par son fournisseur.

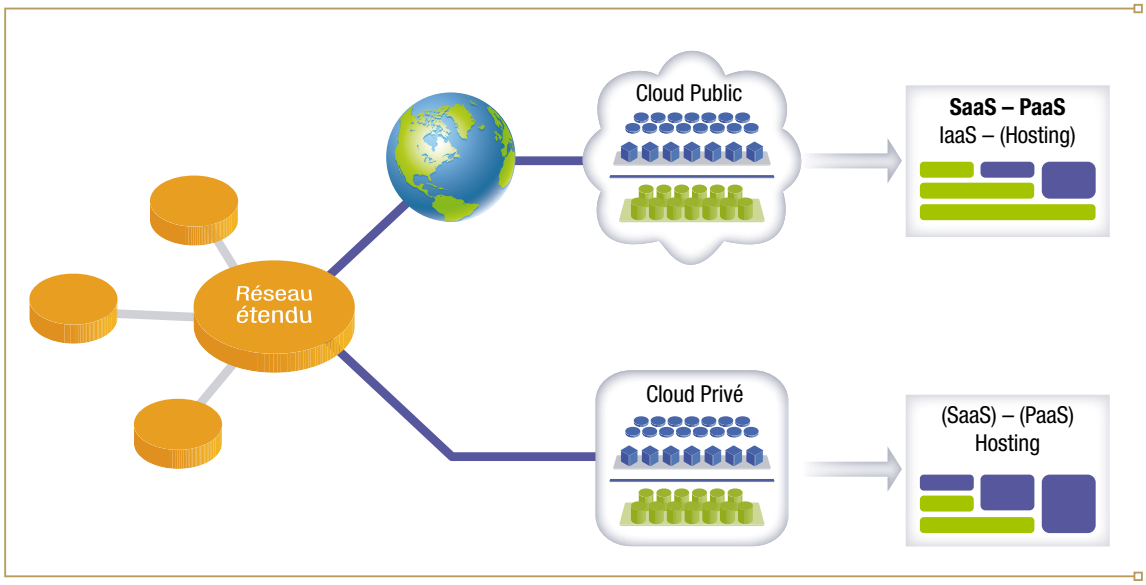


DR

## 2.4. Fixation du prix des services, partage des revenus

Le marché du Cloud est aujourd'hui essentiellement dominé par l'offre et basé sur un modèle économique «à l'usage». Mais comment s'établit la fixation des prix de services et le partage des revenus ?

Ils doivent répondre à deux enjeux principaux :
- Modèle de tarification répondant aux besoins (lisibilité)
- Flexibilité / prédictibilité




DR

### 2.4.1. Structures de prix

- **SaaS :** le plus souvent bâti sur une tarification à l'utilisateur ou au poste intégrant d'une part le prix de base et d'autre part des options (fonctionnalités)

- **PaaS :** variation de tarifs en fonction de l'environnement et des outils disponibles (sous licences ou en open source).

- **IaaS :** tarification très variable s'appuyant sur des prix au serveur virtuel (VM : Virtual Machine – machine virtuelle) ; à la puissance consommée ; à l'heure pour la location de VM ; avec une variation de prix si elle est réservée ou pas ; au Go/au To notamment dans le cadre des offres Cloud Storage ; au volume de données échangées ; etc.

Le choix du modèle de facturation est l'une des clés de voûte de la maîtrise des coûts. Les offres cloud tendent à multiplier, à l'instar des pratiques de la téléphonie mobile, les unités d'œuvre, options, forfaits, extensions, etc. Il devient difficile de comparer les offres SaaS/IaaS/PaaS entre elles. On privilégiera des solutions avec un modèle de facturation articulé autour d'éléments fixes et permettant d'avoir un gain durable sur le couple Capex – Opex.

Toutes les offres ne permettent pas tous les avantages. À titre d'exemple : un grand compte français dans le domaine de l'énergie a récemment constaté qu'entre les coûts « nominaux » d'un grand fournisseur international d'IaaS et la réalité du coût complet, l'écart était de 1 à 3. La raison ? Une facturation peu coûteuse par machine virtuelle, mais des coûts très élevés de transferts de données depuis et vers l'infrastructure du fournisseur.

#### Une prime aux « grands » Data Centers ?

**On a constaté qu'un centre de données composé de 100 000 serveurs affiche un coût total de possession (TCO) inférieur de… 80 % par rapport à celui d'un centre de données de 1 000 serveurs ! La facture d'électricité représente 15 à 20 % du coût total de possession. Un prestataire international de Cloud jouera donc sur les implantations de ses Data Centers afin de rechercher d'obtenir les meilleures conditions avec les fournisseurs d'électricité locaux. De plus, les opérateurs de grands centres de données bénéficient souvent d'importantes remises sur le matériel, de l'ordre de 30 %. L'homogénéité de l'infrastructure permet aussi de réaliser de nettes économies d'échelle. Enfin, en cas d'adoption d'un modèle mutualisé, plus le nombre de locataires est grand, plus les coûts d'administration des applications et de serveurs par locataire diminuent.**

### 2.4.2. Flexibilité et prédictibilité

Il est important de prendre en compte l'ensemble des coûts directs : une solution d'IaaS peut nécessiter des coûts de services (Cloud ou non) supplémentaires pour le SSO (Single Sign On : unification des identifiants et mots de passe), l'antispam, la supervision de la sécurité, ou pour les solutions de provisionnement (provisioning).

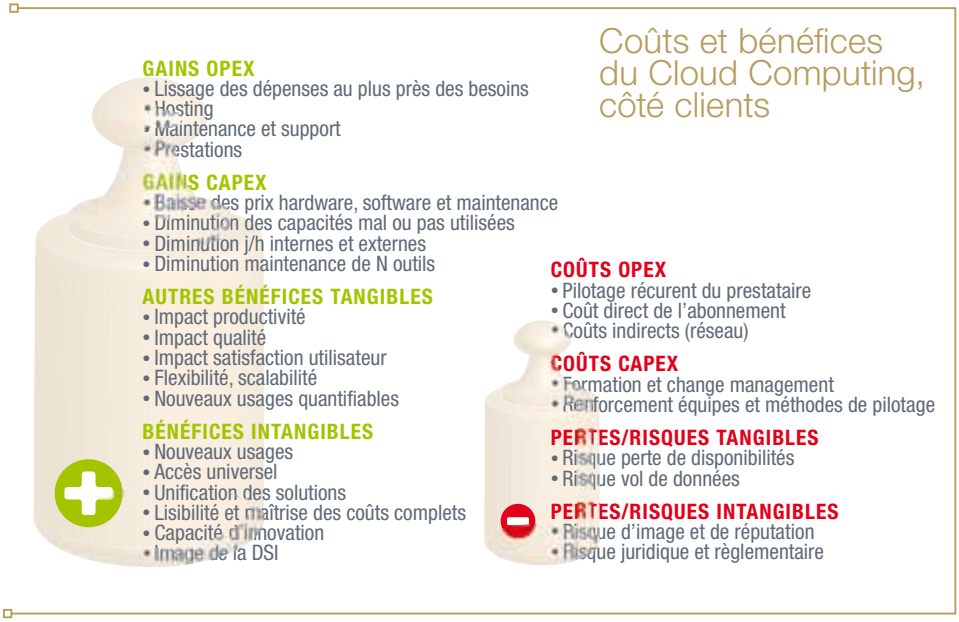
- Les changements technologiques
- Les critères de volume de toute nature : nombre de VM, d'applications, de données, etc.

Le service et notamment les efforts qu'il faudra consentir pour l'industrialiser, afin de maintenir un niveau de flexibilité et de réactivité optimal.

Dès lors que le Cloud devient l'une des briques du reste du système d'information, il faut donc considérer ces modèles de tarification pour les intégrer au modèle cible. En effet la problématique du DSI réside dans le fait de rendre lisibles ses coûts par sa DG et ses clients internes ou externes. La multiplicité des modèles rend cette construction souvent complexe et imposera tôt ou tard une approche en unités d'œuvre qui pourront alors être partagées au-delà même de l'entreprise, par ses fournisseurs et ses partenaires.

## 2.5. Côté clients, dépenses en capital ou dépenses opérationnelles ?

Pour une PME ou une TPE, le Cloud Computing offre plus qu'une baisse de coûts : il permet l'accès à des solutions informatiques jusque-là réservées à des comptes d'une taille largement supérieure. Pour les ETI (Entreprises de taille intermédiaire) et les grands comptes, la « valeur sur investissement» est évidemment plus complexe à déterminer.




DR

## Avantages et inconvénients des modèles cloud, vus par les clients

| | Avantages | Inconvénients |
|---|---|---|
| **Cloud public** | • Mutualisation => Prix | • Sécurité • Accompagnement |
| **Cloud privé** | • Sécurité<br>• Adéquation au besoin | • Investissement (=> coût)<br>• Compétence nécessaire |
| **Cloud privé externalisé** | • Mutualisation • Sécurité, disponibilité<br>• Accompagnement | Nécessite des SLAs de bout en bout (choix du prestataire) |

Traditionnellement, la possession en propre de ses moyens informatiques – qui ressortent donc du Capex – est la règle. Pour certaines entreprises, cet investissement en capital reste tout à fait justifié au regard de leur stratégie financière générale. Le Cloud permet de faire basculer ces investissements ainsi que la composante exploitation du service du côté de l'Opex, ce qui constitue une approche intéressante pour des entreprises de taille moyenne ou avec une trésorerie limitée et dont l'informatique n'est pas le métier principal.

Cette conversion au tout-Opex n'a toutefois pas que des avantages. Pour les sociétés cotées, qui se doivent de présenter des indicateurs financiers conformes aux attentes des actionnaires et investisseurs, le modèle « as a service » peut avoir un effet néfaste sur le bilan. En effet,

## Cloud privé : modèles de facturation

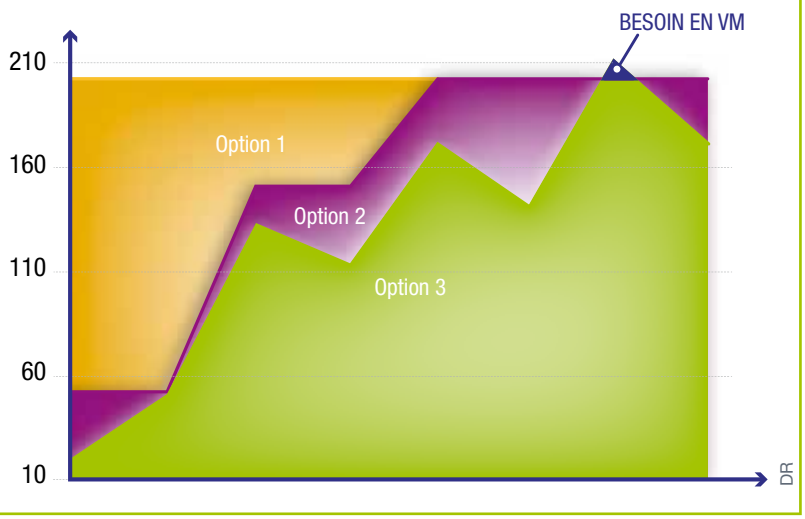
**Détaillons différentes options pour la mise en place d'une IaaS (Infrastructure as a Service) comportant – par exemple – 200 machines virtuelles (VM) dans un premier temps, puis une croissance planifiée.**

**Option 1 : vous construisez votre Cloud privé au sein de vos infrastructures. C'est-à-dire que vous pouvez uniquement bénéficier, si le vendeur vous le permet, d'un achat à l'usage (une location) de vos investissements. La maille de votre loyer risque d'être assez importante (probablement les 200 VM) et pas de capacité variable à la baisse.**

**Option 2 : le partenaire installe une infrastructure Cloud dans votre Datacenter. Cette infrastructure peut vous permettre d'avoir une maille plus petite (par exemple pour 50 VM) et vous permettre, sous certaines conditions, de faire varier la capacité à la hausse mais plus difficilement à la baisse.**

**Option 3 : vous n'êtes plus au sein de vos infrastructures et vous construisez un Cloud privé chez un partenaire. Compte tenu de ses capacités de mutualisation, vous bénéficiez des possibilités du Cloud. Facturation à la VM, en fonction de votre besoin, à la hausse comme à la baisse.**

**Pour un exemple de besoins, voici ce que les différents scénarios donnent. L'option 3 est confondue avec les besoins en VM qui, au-delà de l'aspect économique, permet de répondre aux pics.**



l'Opex impacte l'Ebitda (excédent brut d'exploitation), alors qu'un achat en Capex s'amortit sur l'Ebit (résultat d'exploitation).

## 2.6. Les bonnes questions à se poser en termes de valeurs tangibles et intangibles, selon eSCM

Avec l'élasticité des ressources, le Cloud apporte une réponse pertinente à la question de la prévisibilité des besoins. Mais se pose, en retour, la question de la prévisibilité des coûts. Car la grande souplesse d'une utilisation à la demande va de pair avec le risque de ne pas savoir estimer à l'avance ses besoins réels, et donc de se retrouver confronté à des factures bien plus élevées que prévu. Les processus outillés de gestion de la capacité, côté client et fournisseur, sont à cet égard essentiels à mettre en œuvre.

Le référentiel propose des pratiques structurées pour piloter économiquement le Cloud Computing, du point de vue du client :
**Manager le modèle économique sur le cycle de vie complet d'un service.**

Le coût (et les bénéfices) d'une solution Cloud Computing ne peuvent se résumer à son prix « frontal », fut-il très attractif, et un projet Cloud mal mené peut se traduire par une hausse des coûts, parfois sévère.

eSCM recommande d'établir et de faire vivre un business case permettant d'évaluer, tant en amont que périodiquement pendant la vie du service, les coûts et bénéfices de façon plus complète, en intégrant :

- **L'évolution de la demande :** certaines solutions sont très avantageuses pour un petit nombre d'utilisateurs et pour les services de base. Mais elles le deviennent moins quand on grandit ou qu'on augmente le nombre de modules. A contrario, d'autres «cas d'usages» peuvent apparaître et doivent être intégrés et valorisés dans le business case.

- **Les bénéfices et coûts indirects et internes :** l'atténuation ou la réduction de certains risques clés, le renforcement des infrastructures éventuellement nécessaires (ex : WAN), les coûts de management récurrents, les coûts d'adaptation des solutions aux besoins, etc. sont autant de postes de coût qu'il convient d'évaluer sur la durée. À titre d'exemple, il est estimé que le coût de pilotage d'un service externalisé représente, en moyenne et sur 3 à 5 ans, 15 à 20% de la facture fournisseur globale.

La tarification doit pouvoir suivre l'évolution des besoins des utilisateurs (SaaS) ou administrateurs/développeurs (IaaS). Pour cela elle doit intégrer dès la contractualisation, les critères pouvant impacter le prix et ainsi prendre en compte :

- **Les bénéfices et coûts de transition :** les bénéfices provenant d'une allocation automatique plus rapide (IaaS), la réduction des

coûts de mise en place (setup) et l'accélération des cycles projets (SaaS) sont également à intégrer… au même titre que les coûts de transition vers le Cloud, de conduite du changement, d'adaptation des process/savoir-faire opérationnels et de pilotage, de préparation et de réversibilité.

eSCM agrège le pilotage économique « *stricto sensu* » (le ratio bénéfice/coût complet évoqué plus haut) à un management plus complet par la valeur, intégrant bénéfices et coûts intangibles ou non monétaires.

Reste à accéder aux centres d'hébergement : c'est là qu'on retrouve les télécoms. Après avoir choisi le bon niveau d'externalisation, il faut choisir le bon modèle d'intégration dans son réseau d'entreprise : réseau privé pour Cloud privé (et très rarement réseau public), réseau public – Internet – pour Cloud public (et très rarement réseau privé).

Les tableaux suivant listent quelques-unes des opportunités de création de valeurs, pour les clients et pour les fournisseurs.

### 2.6.1. Tableau récapitulatif côté clients

| Catégorie | Caractéristiques des offres cloud | Valeur intangible / indirecte |
|---|---|---|
| Juste-à-temps / Agilité | Auto-provisionnement (self provisioning) | • Rapidité de réponse aux demandes utilisateurs<br>• Productivité des utilisateurs<br>• Image de la DSI<br>• Coûts internes de provisionnement |
| | Provisionnement rapide | • Diminution des délais de mise en œuvre des projets<br>• Rapidité de mise en œuvre et de réaction aux demandes métiers<br>• Image de la DSI.<br>• Productivité des utilisateurs |
| | Évolutivité (Scalability) | • Adresser de façon optimale les pics de charge<br>• Possibilité d'adapter les coûts à la baisse (nécessite de se doter des processus adaptés) |
| Optimisation des ressources | • Libération de ressources IT vers des tâches à plus forte valeur ajoutée.<br>• Meilleur usage des ressources | • Maîtrise des coûts<br>• Valeur ajoutée et image de la DSI |
| Coûts | • Modèles de tarification fiables et refacturables<br>• Peu ou pas de coûts d'entrée au service<br>• Contrôle des consommations | • Amélioration du pilotage des coûts et investissements de la DSI<br>• Possibilité de déployer des solutions à « l'état de l'art » pour de petits périmètres et d'offrir un portefeuille d'offres différencié… |

•••

...

| Catégorie | Caractéristiques des offres cloud | Valeur intangible / indirecte |
|---|---|---|
| Conformité | • Un risque de manque de transparence<br>• Des propositions intéressantes en matière de Green IT<br>• Réduit la complexité interne | … et, à terme, l'opportunité de déléguer des risques de conformité et de renforcer, par l'émergence de standards et de réglementations plus industrielles, cette conformité<br>• Favoriser le respect des engagements environnementaux et sociétaux |
| Qualité de service | • Accès à des ressources et des infrastructures à haute disponibilité.<br>• Points d'accès distants multiples.<br>• Amélioration du support<br>• Dépendance plus faible envers les « personnes clés » | • Productivité des utilisateurs<br>• Satisfaction des utilisateurs<br>• Satisfaction métier<br>• Accès à un support 24x7, bénéficiant de l'effet d'échelle en matière de compétences. |
| Cohérence technologique et interopérabilité | Une fois les modèles matures, accès à des infrastructures standardisées, dotées d'interfaces ouvertes | • Ce point n'est pas encore matérialisé… il s'agit autant d'un risque que d'une opportunité<br>• Contribution à l'urbanisation du SI<br>• Isolation des domaines |
| Innovation par l'offre | • Provisionnement facile<br>• Accès à des solutions « best of breed » innovantes<br>• Évolutivité des solutions (constamment à jour) | • Capacité à répondre rapidement aux besoins métiers changeants ; soutien des initiatives métier<br>• Moins de risques d'obsolescence des solutions et de dette technique<br>• Favorise la collaboration et l'interconnexion universelle avec les salariés, les clients et les partenaires de l'entreprise |
| Innovation métier | Favorise et accélère la mise en place de nouveaux business model métiers et de nouveaux usages | • Ex : utilisation de solutions sur des activités qui ne pouvaient être financées<br>• Ex : réseaux sociaux<br>• Ex : crowdsourcing, opendata, etc. |
| Différenciation | Apport de fonctionnalités « best of breed » | • Opportunité : disposer des meilleures fonctionalités en continu. Risque : Les clients devront accepter de voir leur informatique dotée de fonctionnalités non-souhaitées ou a contrario, de voir leurs idées nouvelles utilisées par des concurrents.<br>• De nouveaux critères de différenciation devront voir le jour |

### 2.6.2. Tableau récapitulatif, côté fournisseurs

| Catégorie | Caractéristiques des offres cloud | Valeur intangible / indirecte |
|---|---|---|
| Fidélisation client | Le client prend un abonnement dans la durée | • Meilleure lisibilité du CA à moyen terme : 1 client signé c'est 3 ans de revenu au moins<br>• Vente récurrente plus naturelle, moins dépendante de l'évolution de la technologie |
| Conquête de nouveaux clients | Accès universel pour les clients | Service accessible à de nouveaux clients, qui ne pouvaient s'offrir des solutions internes |
| Différenciation | Effet d'annonce, d'image, bénéfices tangibles pour les clients | Effet « innovant » remarqué dans de nombreux secteurs pour les pionniers du SaaS/Cloud, qui conquièrent rapidement des parts de marché au détriment des acteurs historiques |
| Extension de gamme | Capacité à monter et descendre en gamme, à faire évoluer l'offre, à la construire en partenariat | Une offre plus évolutive et plus déclinable |
| Augmentation de la rentabilité | | Observé chez plusieurs acteurs, qui trouvent une source de revenu additionnel dans le fait de proposer l'hébergement SaaS au-dessus de leurs solutions. Dépend du niveau de capture de valeur par les acteurs IaaS au détriment des éditeurs SaaS, et du niveau de concurrence qui s'instaure… |

# 3. UNE NOUVELLE CONTRACTUALISATION

## 3.1. Quels modèles de contrats ?

Pour l'élaboration des contrats – côté clients – voici quelques recommandations :

- Les modèles économiques qui devraient voir le jour ainsi que le grand nombre d'acteurs nécessaires à la fourniture du service renforcent le besoin d'identifier côté fournisseur un responsable unique des engagements. Ce dernier doit afficher les accords qu'il pourrait tisser avec des sous-traitants afin d'éviter une notion de « shadow contract ».

- Les exigences contractuelles du client doivent figurer dès l'appel d'offres, et non être exprimées lors de la négociation finale avec le prestataire retenu. En effet, les contrats types des fournisseurs étant encore très évolutifs, ces contraintes peuvent constituer un critère de choix important entre les soumissionnaires.

- Il est impératif que le contrat laisse de la place à la « souplesse ». Les solutions cloud sont très évolutives, tant dans les fonctionnalités offertes, que par la volumétrie à terme. Le contrat, qu'on l'appelle contrat « relationnel », « agile » ou « co-managé », doit pouvoir parallèlement évoluer.

- Le contrat est un objet « vivant » : une fois signé, il doit être piloté, revu, amendé et le contrôle de son application (notamment via les

### Cahier des charges, appel d'offres et contractualisation


1. Business case
   Options retenues
2. Plan projet
   Quel service voulons-nous obtenir ?
   Comment choisir le fournisseur ?
   Sur quels critères ?
   Préparer les exigences (RFI, RFP)
3. À qui envoyer la consultation ?
   Collecter les réponses
   Dépouiller, analyser
   Choisir le(s) finalite(s)
4. Comment négocier ?
   Confirmer l'existent
   Négocier
   Rédiger contrats, SLA
5. Trasmettre les exigences
   Planifier – Spécifier
   Définir – Recetter – Déployer
6. Du service
   Des ressources – Des équipes
   Des connaissances
   Faire la recette du service

DR

audits et benchmarks) revêt une importance plus grande dans le contexte du Cloud que jusqu'alors.

- De manière générale dès lors que les données quittent le territoire national, il faut s'interroger sur la juridiction compétente. Si nécessaire, le fournisseur devra pouvoir s'engager sur des zones géographiques de stockage et fournir au client une analyse de risques de ces lieux aussi bien d'un point de vue géographique, règlementaire que géopolitique. À titre d'exemple : les États-Unis ont instauré après l'attentat du 11 septembre 2001 la loi du Patriot Act : il existe un risque que les données soient exploitées à une autre fin un autre but que celle recherchée par cette loi. Comment garantir que les données ne sont pas utilisées à des fins commerciales ou stratégiques ?

- De nombreux pays, en particulier européens, sont conscients de ces risques, d'où l'intérêt porté à des offres « nationales », qu'elles soient portées par des « champions nationaux » ou par des implantations locales de groupes étrangers.

- La sécurité constitue un autre point majeur. Il s'agit ici de limiter le risque de perte de données, d'utilisations frauduleuses et d'atteinte à leur intégrité. Le fournisseur doit présenter les mesures prises pour la lutte contre les attaques virales ou les cyber-attaques. Le fournisseur prouvera également que son plan de continuité d'activité couvre bien le périmètre du client. En cas de déclenchement de ce plan, le contrat précisera également qui, du client ou du fournisseur, gère la crise.

Le modèle cloud apporte des réponses/solutions là où les modèles traditionnels étaient bloquants :

- **Durée des contrats :** là où les contrats IT étaient généralement de 12 à 36 mois, mais rarement moins, on peut, grâce au Cloud, avoir des services contractualisés pour quelques semaines…

- **Évolutivité des contrats :** un service avait un périmètre donné et n'évoluait que via des avenants au contrat (impossible ou coûteux de diminuer le dimensionnement après coup, par exemple). Le Cloud transforme la manière d'envisager les contrats et leurs évolutions.

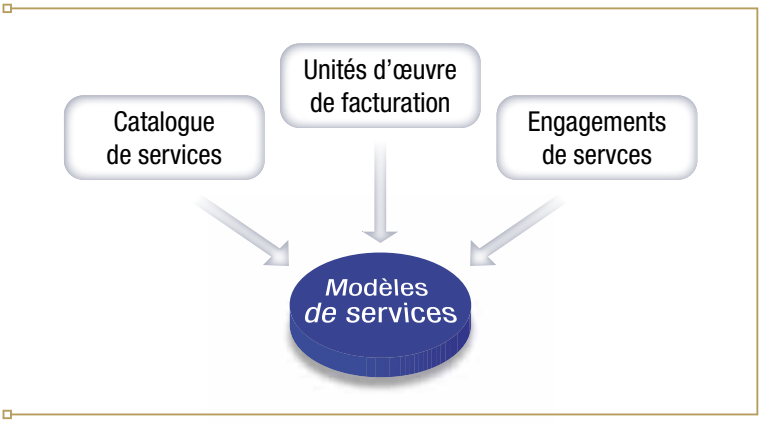
- **Achats :** les services achats sont moins impliqués et tous les acteurs métiers peuvent être acheteurs – cela apporte de la flexibilité mais est plus « risqué ».

- **Engagement et qualité de services :** le Cloud implique une qualité de services nécessairement liée à celles des opérateurs ; ceux-ci s'engagent à une disponibilité de service indispensable aux applications critiques notamment.

- **Réactivité, flexibilité :** ils deviennent réalité et ce faisant, exprimables contractuellement.

**Et la contractualisation avec les utilisateurs ?**
Comme dans la relation entre DSI et fournisseurs, un modèle de services doit régir la relation entre la DSI et ses utilisateurs. Ce type de modèle repose sur des engagements de résultats et décrit de façon très précise :

- Le catalogue des services contractuels : description technique, modalités de réalisation, dépendances, criticité,
- Les engagements associés à chacun des services,
- Les unités de facturation.



DR

Le modèle de services se traduit concrètement par les trois documents contractuels fondamentaux que sont :

- Le contrat : les services, les obligations mutuelles, les unités de facturation.
- Le PAQ (Plan d'Assurance Qualité) et le PAS (Plan d'Assurance Sécurité) : la répartition des responsabilités dans la relation quotidienne.
- Les conventions de services (Service Level Agreement/Operation Level Agreement) : engagements de services et modalités de mesure.

## 3.2. Engagements de service et de niveaux de service

Le contrat doit s'appuyer sur un catalogue de services clairement définis, chaque service étant adossé à des engagements de niveaux de service (SLA) clairs.

Le Cloud Computing – grâce notamment aux apports des environnements virtualisés et de la redondance qu'ils permettent – bénéficie intrinsèquement d'une disponibilité plus élevée qu'un hébergement classique. Toutefois des SLA élevés ne sont bien sûr nécessaires que pour répondre à des enjeux critiques. Il ne s'agit pas de tomber dans la sécurisation et la fiabilisation à tout prix. Tous les usages ne nécessitent pas un taux de disponibilité maximal. Aussi, à l'intérieur d'un même catalogue de services, ou en panachant différentes offres, le DSI

va avoir à sa disposition une palette de solutions, avec des caractéristiques et des tarifs différents. À lui de mettre en relation l'offre et ses différents types de besoins, pour choisir le meilleur de chaque technologie en fonction de ses enjeux.

Une fois les SLA définis, le contrat doit prévoir les moyens de les mesurer. La difficulté traditionnelle est que le DSI doit pouvoir garantir les SLA du service global, et pas seulement ceux de la plate-forme cloud, là où le prestataire ne s'engage que sur son domaine de responsabilité. Le Cloud est indissociable de l'accès au Cloud. À quoi sert d'avoir une application totalement disponible si les utilisateurs ne peuvent y accéder, faute d'une infrastructure d'accès suffisamment redondée ? C'est pourquoi les SLA doivent être envisagés de « bout en bout ». (voir encadré « Nécessité de la mesure » page précédente).

## 3.3. Contractualisation du Cloud : entretiens croisés avec deux avocates

Maîtres Olivia Flipo (OF Avocat) et Mahasti Razavi (August & Debouzy) – toutes deux en pointe sur les problématiques juridiques du Cloud Computing – ont accepté de répondre à nos questions.

**Syntec Numérique : En ce début d'année 2012, les opérateurs de Cloud Computing (SaaS, PaaS et/ou IaaS) proposent-ils selon**

### Nécessité de la mesure

**Afin de concilier Cloud Computing et Qualité de Service, il apparaît nécessaire de disposer d'un système de mesure fiable et impartial.**
**Une première approche – issue du monde réseau et qui ne dépaysera personne dans un environnement « télécoms » – consiste à mettre en place des méthodologies de test au niveau protocolaire (IP ou Ethernet). Cette approche reste toutefois aveugle aux problématiques des « couches hautes », souvent à l'origine des éternels débats et incompréhensions entre DSI et utilisateurs. Mieux vaut donc une vision plus « applicative » qui se rapproche du ressenti de l'utilisateur derrière son poste de travail (on parle alors de « QoE – Quality of Experience »).**
**Ici des « robots » vont analyser l'intégralité de la « pile applicative », en continu, aussi longtemps que nécessaire. Les problèmes réseaux seront décelés, mais aussi ceux des couches hautes, invisibles par les approches précédentes. On pourra alors déterminer quel « espace réseau » est fautif dans la dégradation de la qualité perçue par les utilisateurs, et quelles sont les raisons de cette dégradation.**
**L'entreprise construira des indicateurs pertinents pour ses applications cloud, lisibles de tous, facilitant la contractualisation sur la base d'engagements de services qui font sens.**
**Il lui faudra toutefois surmonter un dernier obstacle : les deux « espaces réseaux », ainsi que l'environnement Cloud sur lequel l'application cible est opérée n'utilisent pas, jusqu'à plus ample informé, les mêmes référentiels de Qualité de Service.**
**Les indicateurs des différents prestataires de la chaîne de services sont présentés sous des formes distinctes par chaque acteur – empêchant une lecture homogène des tableaux de bord et des engagements contractuels. Même si l'entreprise aspire à disposer d'une vision unifiée de la Qualité de Service des applications cloud, le chemin est encore long avant que cette visibilité ne soit délivrée de façon homogène, impartiale, exploitable directement et simultanément par l'ensemble des fournisseurs.**

**vous des contrats juridiques stabilisés pour les deux parties ?**

***Mahasti Razavi :*** *Un contrat est nécessairement stable au moment de sa signature par les parties dans la mesure où il comprend les conditions dans lesquelles l'utilisateur et l'opérateur de Cloud Computing ont décidé de fixer leur accord. Cet accord qui certes fige les relations des parties peut prévoir une série d'évolutions au cours de son exécution tenant par exemple à l'évolution du périmètre de l'utilisateur couvert par le contrat ou des textes législatifs. Il est intéressant de noter que les marges de manœuvre de négociations de ces contrats vont fondamentalement dépendre de la nature de l'offre cloud concernée, publique ou privée.*

*En dehors de cette phase de stabilité, il est parfaitement naturel qu'un contrat type ou une base contractuelle standardisée évolue avec le développement de la pratique, la maturation des offres de cloud computing, le développement de la concurrence en la matière, l'évolution des besoins des utilisateurs, ainsi que les évolutions juridiques tant réglementaires que jurisprudentielles. Ainsi, un utilisateur ayant conclu un contrat en 2011 ne devra pas être surpris si dans 3 ans, le contrat qui lui est proposé pour un service similaire est différent du contrat qu'il aura pu conclure. Le nouveau contrat sera alors conforme aux règles de l'art du moment.*

***Olivia Flipo :*** *En effet, les contrats ne font que refléter le niveau de maturité de l'offre commerciale et la qualité technique de la solution et du service vendus. Les spécificités des contrats de fourniture de services en mode SaaS sont bien définies aujourd'hui. Les contrats assurent un équilibre entre contraintes et équilibre financier du fournisseur et attentes du client. Il n'en demeure pas moins vrai que certains contrats comportent de nombreuses lacunes tant pour le client que pour le prestataire. Ceux-ci pourraient être renforcés sur certains aspects fondamentaux (disponibilité, sauvegarde, accès à la solution etc.) et/ou clarifiés (localisation des serveurs, confidentialité des données, réversibilité…).*

*De plus, de nombreux éditeurs fournisseurs de SaaS dépendent directement des niveaux de services (SLA) de leurs hébergeurs ou fournisseurs IaaS. Leur niveau d'engagement concernant notamment la sécurité ou la disponibilité sera conditionné par les SLA de l'hébergeur. Pour caricaturer, ils maîtrisent directement la « solution logicielle », mais indirectement le « service ». Pour autant, vis-à-vis du client final, ils sont responsables : à charge pour eux de se retourner contre l'hébergeur. Leur responsabilité est donc accrue et nous ne pouvons que leur conseiller de choisir des hébergeurs avec lesquels un véritable partenariat sera possible, avec la possibilité d'adapter les SLA en négociant les conditions des contrats d'hébergement. Si ce n'est pas possible, le fournisseur devra répercuter les niveaux de services de l'hébergeur et les limitations de responsabilité afin d'exclure les risques qu'il ne maîtrise techniquement et concrètement pas (ralentissement et coupure du réseau Internet, panne électrique entre autres, sécurité physique et logique des serveurs).*

*Par ailleurs, les données à caractère personnel communiquées à des sous-traitants, tels les hébergeurs, doivent bénéficier de garanties de sécurité en application de la loi Informatique et Libertés. Dès lors, les contrats liant l'éditeur de solution SaaS aux hébergeurs ainsi que les*

> « ***Il n'est pas anormal*** *que les engagements sur les niveaux de services ne soient pas identiques entre opérateurs de Cloud Computing puisque chaque offre peut être différente en fonction des produits concernés.* »

*contrats liant l'éditeur et les clients, utilisateurs doivent, tous deux, prévoir une clause spécifique couvrant la confidentialité et l'intégrité des données ainsi confiées. L'éditeur et le client final devront aussi prendre des dispositions (audits de sécurité) afin de s'assurer de l'effectivité des garanties offertes par l'hébergeur en matière de protection des données.*

**Syntec Numérique : Quels sont les principaux points juridiques de vigilance – spécifiques au Cloud Computing – que vous mettriez en exergue et qui doivent faire objet d'attention particulière dans le contrat ?**

***Mahasti Razavi :*** *Les questions récurrentes et légitimes des utilisateurs portent majoritairement sur la sécurité/confidentialité, les niveaux de services et l'audit de l'opérateur de Cloud Computing. Certains s'interrogent également sur la réversibilité qui est un sujet très opérationnel mais que les contrats doivent évoquer.*

*Pour ce qui est de la confidentialité/sécurité (il s'agit de thématiques juridiques distinctes mais complémentaires, prises ici dans leur ensemble), les prestataires reconnus du marché sont précisément (et par nature) au cœur des règles de l'art si ce n'est les fondateurs mêmes desdites règles : ils sont les « sachants » et leur expertise est souvent supérieure en la matière à celle des utilisateurs. Cela étant, il est naturel de s'assurer que l'opérateur de Cloud Computing respecte la sécurité et la confidentialité des données qui transitent et sont stockées par son intermédiaire, respecte les textes de loi (tels que modifiés éventuellement pendant la durée du contrat) et que ceci constitue un engagement contractuel clair de sa part. S'il est un point d'attention particulière pour les entreprises, c'est bien de savoir si le prestataire propose ou non les « model clauses » décidées par la Commission européenne en 2010. Il est clair qu'il faut privilégier le contrat comprenant cette garantie importante.*

*Une fois ce principe énoncé, les contrats pourront être nuancés en fonction notamment des applications proposées en cloud, de la nature des données qui transitent et sont stockées, etc…*

*La question du niveau de service constitue un sujet central, certes opérationnel avant tout mais que le contrat doit également aborder de manière précise tant en ce qui concerne le périmètre d'engagement, les mécanismes de calcul de respect ou de non-respect des niveaux, la conservation des éléments de preuve, les conséquences en cas de non-respect de ces engagements de même éventuellement que les mécanismes d'escalade en cas de désaccord entre les parties. Il convient de garder en mémoire qu'il n'est pas anormal que les engagements sur les niveaux de services ne soient pas identiques entre opérateurs de Cloud Computing puisque chaque offre peut être différente en fonction des produits concernés, des éléments financiers négociés sans oublier que ces éléments varieront de manière importante selon que l'utilisateur souhaite bénéficier d'un Cloud public, privé ou hybride.*

*L'audit est également une demande fréquente des utilisateurs, même le souhait de certains utilisateurs peut paraitre irréaliste en pratique : on ne peut imaginer tous les clients d'un même Cloud envoyer leurs auditeurs quand ils le souhaitent (et même après un préavis raisonnable)*

*scruter/analyser les serveurs de l'opérateur sur lesquels pourraient se trouver les données – confidentielles – d'autres clients... sans oublier les rencontres intempestives entre tous les auditeurs de tous les utilisateurs puisque la vocation première du Cloud, du moins public, est la mutualisation des serveurs. Encore une fois, si le besoin des utilisateurs est parfaitement légitime, et que le contrat doit tenir compte de cet aspect, il convient de prévoir des dispositions contractuelles qui reflètent les cas d'espèce et en particulier la nature du Cloud (public, privé, hybride). Dans certains cas, une procédure d'auto-audit peut être parfaitement adaptée.*
*Quelques mots sur la réversibilité que l'on oublie pourtant parfois puisqu'elle concerne la fin de la relation contractuelle. A notre sens, un utilisateur doit d'abord comprendre ce qui se passe en pratique à la fin du contrat selon le type de Cloud et la nature du service proposé et s'assurer que le contrat définit les conditions dans lesquelles il pourra reprendre (ou faire reprendre) la main sur ce qui a un temps fait l'objet du Cloud qui a expiré ou a été résilié.*

***Olivia Flipo :*** *Je confirme l'aspect primordial des engagements de niveaux de services (SLA). Du point de vue des fournisseurs (éditeurs, hébergeurs et cloud providers), ces engagements représentent un avantage concurrentiel certain, à condition qu'ils soient rédigés de façon claire et précise. Une exigence qui s'applique autant aux fournisseurs de SaaS que de IaaS ou de PaaS. Les SLA doivent a minima prévoir et décrire :*

- *Le niveau de performance du service (hors Internet),*
- *Le niveau de disponibilité du service avec les critères (métriques) de mesure voire les modalités de reprise après sinistre,*
- *Les mesures destinées à assurer la sécurité et la confidentialité mises en place (accès à la solution, système redondant, sécurité logique et physique des serveurs).*

*Deuxième point d'attention, trop souvent éludé, la question de la réversibilité et de l'assistance du fournisseur devrait être abordée dans le contrat. Elle répond à un besoin croissant des clients finaux concernant la continuité ou la souplesse du service et la récupération des données. Dans ce même ordre d'idée, et lorsque la solution logicielle métier le permet, le contrat devrait prévoir une évolution de l'application. Ce dynamisme caractérise le Cloud.*
*Enfin, les responsabilités respectives du fournisseur de solution SaaS et de l'utilisateur doivent être établies. Ainsi l'utilisateur doit s'engager à mettre en place des mesures techniques de sécurité et à respecter les procédures d'accès.*
*Dernière remarque, il est recommandé de définir contractuellement la loi applicable et les tribunaux territorialement compétents et particulièrement, dans l'hypothèse où les données pourraient être hébergées sur des serveurs localisés hors de France L'objectif est d'éviter qu'en cas de litige, ce soit la loi du pays où se trouvent les serveurs qui s'applique. De plus, le client doit connaître la localisation des serveurs pour être en mesure d'effectuer les déclarations nécessaires auprès de la CNIL et d'informer les personnes concernées conformément à la loi Informatique et Libertés.*

**Syntec Numérique : Comment s'y prendre concrètement – vers qui se tourner et pour quoi faire – pour que les aspects juridiques ne soient pas un frein à l'utilisation du Cloud Computing dans les entreprises ? Et par la suite, qu'ils ne grippent pas le bon déroulement opérationnel du contrat ainsi que ses évolutions éventuelles ?**

***Mahasti Razavi :*** *Indéniablement, le sujet du Cloud peut paraitre sensible. Il touche énormément d'acteurs et d'intérêts nationaux comme internationaux et est en pleine évolution d'un point de vue technique, marketing, commercial et règlementaire/juridique. Il y aura bien sûr de nouvelles normes juridiques qui viendront impacter le Cloud mais, pour autant, tous les jours des contrats sont signés satisfaisant à la fois les utilisateurs et les opérateurs. C'est la preuve qu'il n'y a pas de « frein » au développement et à l'usage du Cloud si les acteurs impliqués dans les discussions maitrisent cette thématique et s'engagent sur des bases de transparence en particulier sur la question de la protection des données.*

*C'est pourquoi la conclusion d'un contrat Cloud se prépare grâce à des équipes de travail transverses impliquant notamment les DSI, les métiers, les achats, ainsi que les juristes et les avocats.*

***Olivia Flipo :*** *S'agissant d'un contrat de services complexe (licence, maintenance, assistance, formation…) dont l'exécution suppose l'intervention de plusieurs fournisseurs (hébergeur, éditeur, intégrateur, VAR, opérateur télécom…), il est vrai que de nombreux aspects doivent être abordés, validés et repris dans le contrat. Lors de la mise en place de nouvelles offres en mode SaaS, il faudra intégrer un juriste dès le début de la réflexion. De cette coopération naîtra souvent un contrat plus complet et plus sûr. Évolutif, répondant aux exigences légales, il fondera une relation pérenne. La rentabilité du Cloud repose sur un calcul fondé sur différents éléments : un prix minimal, des prix d'utilisation variables selon la durée et le périmètre d'utilisation. Il est possible – et sans doute judicieux – de proposer au client une phase d'essai gratuit à laquelle pourrait succéder le contrat. Enfin, les fournisseurs de Cloud Computing doivent impérativement disposer d'un contrat d'assurance adapté à leur activité. Je conseille à chaque entreprise de vérifier très attentivement les exclusions de garanties et les niveaux de garantie.*

> ***« Le client doit connaître*** *la localisation des serveurs pour être en mesure d'effectuer les déclarations nécessaires auprès de la CNIL et d'informer les personnes concernées conformément à la loi Informatique et Libertés. »*

## 3.4. Cloud Computing et Qualité de Service

Gérer la qualité de service « perçue » par un utilisateur de Cloud Computing est un réel défi. Pour accéder à un Cloud « public » (ce qui est le cas pour la majorité des applications en mode SaaS par exemple) il faut, à un moment ou un autre, emprunter Internet, qui n'a jamais fait bon ménage avec la Qualité de Service. Pour schématiser, l'utilisateur final doit traverser, pour atteindre son service cloud, deux « espaces réseau » de nature distincte :

- Son propre réseau (étendu) d'entreprise, au sein duquel la gestion de la Qualité de Service est une opération de routine, maîtrisée à la fois par les opérateurs télécoms, les intégrateurs, les acteurs spécialisés, voire l'entreprise elle-même.

- Le réseau qui sépare ce premier réseau du lieu d'hébergement du service cloud en question, c'est-à-dire Internet dans la plupart des accès à un Cloud « public ». Ici, la mise en place de mécanismes de gestion de la Qualité de Service se révèle nettement plus délicate.

Des solutions existent cependant. Certaines nécessitent le déploiement d'équipements aux extrémités. D'autres, récentes, se basent sur une interconnexion plus ou moins directe entre l'infrastructure du fournisseur de Cloud et celle de l'utilisateur final. Toutes ces offres promettent une « Qualité de Service » retrouvée, même « de bout en bout » – encore faut-il savoir de quel « bout » on parle ! En la matière, bien souvent, les indicateurs diffèrent, les engagements aussi.

**Il faut faire très attention** aux standards utilisés, notamment aux interfaces de programmation ou à l'aspect propriétaire des formats de données.

## 3.5. De la réversibilité en matière de Cloud

La problématique de réversibilité est spécifique dans un modèle de Cloud. Classiquement, la réversibilité intègre le transfert de quatre éléments clés : les ressources (physiques et propriété intellectuelle), les connaissances nécessaires pour faire fonctionner le service, les personnels et le service proprement dit.

Dans le cas d'offres cloud, le transfert de personnel est évidemment hors sujet ; celui des actifs physiques également, sauf exception. Reste deux points clés : le transfert du service et celui des données (structurées et non) : images de machines virtuelles, environnements de programmation, données applicatives, règles métiers, paramétrages… et là, la situation peut s'avérer très délicate. Il faut faire très attention aux standards utilisés, notamment aux interfaces de programmation ou à l'aspect propriétaire des formats de données. Certains fournisseurs utilisent des langages propriétaires ou des variantes de standards existants (Java, etc.) induisant un verrouillage de fait du client.

Les clauses contractuelles doivent être étudiées de près : certains fournisseurs limitent abusivement les volumes et le débit des transferts d'information en cas de réversibilité, pouvant rendre celle-ci impossible dans les faits. Les bonnes pratiques eSCM couvrent le sujet de façon étendue et peuvent fournir une aide sur les sujets clés de la réversibilité, allant des responsabilités des parties à la construction et au maintien du plan et à l'exécution de la réversibilité.

### 3.5.1. Rester vigilant sur le risque de capture de la valeur

Dans le modèle du Cloud Computing, le client perd la propriété et le contrôle des actifs techniques et des applications. Pour de nombreuses raisons, la réversibilité complète d'une solution IaaS ou SaaS est fortement sujette à caution. De ce fait se pose un risque exacerbé, pour le client, de se retrouver plus que jamais prisonnier d'un prestataire, et dépendant du bon vouloir de celui-ci en matière de tarification et de valeur ajoutée. Le client avisé aura un intérêt majeur à maintenir entre plusieurs prestataires une saine concurrence afin de prévenir les abus de position.

## 3.6. Comment structurer la contractualisation, selon eSCM ?

Le référentiel eSCM apporte une aide significative pour structurer (côté client comme côté fournisseur) la consultation et la contractualisation d'un projet de Cloud en fournissant notamment des checklists de plus de 50 items composant les 20 ou 30 clauses-clés d'un contrat. Citons notamment :

| Clauses clés | |
|---|---|
| La juridiction et le cadre légal/réglementaire applicable | Avec une vigilance particulière sur le choix de territorialité des accords, eu égard notamment au Patriot Act américain. |
| La définition des services attendus | Et les conditions d'évolution du catalogue de services. |
| La définition des engagements de services et des services annexes (ex : support, provisionnement) | Avec notamment une certaine vigilance sur les clauses limitant par exemple la capacité à décommissionner ou réinternaliser certains services. |
| L'intégration technique/ l'interopérabilité/les standards techniques | Et l'obligation de conformité aux normes existantes et/ou émergentes, ou de témoigner et reporter sur ces sujets. |
| Modèle de gouvernance : rôles, activités, autorité, interfaces, responsabilités, comités | Sujets « relativement » classiques. Attention à l'appontage des processus de service management. |
| Auditabilité | Une exigence très forte, à avoir notamment vis-à-vis des acteurs américains – ex : audit SAS 70. |
| La sécurité (intégrité, accès, confidentialité, …) et la propriété intellectuelle ou physique | Propriété des données, mais aussi des procédures et/ou connaissances produites à l'occasion du contrat par exemple, propriété des actifs transférés, des machines virtuelles et de leur paramétrage |
| La transition | |
| La réversibilité et la gestion des connaissances | |
| La continuité des services | |
| Les conditions tarifaires | Pour lesquelles une attention particulière sera prêtée aux effets de bord, unités d'œuvre, etc… des clauses de « devoir d'alerte » en cas de consommation anormale, peuvent par exemple être prévues. |

# 4. MODÈLES D'ACTIVITÉS

## 4.1. Évolution de la chaîne de valeur

Le Cloud apporte des modifications profondes du positionnement des acteurs de l'IT sur deux chaînes de valeur distinctes :

- «***Cloud Enablement***» : Création, construction et management de services cloud
- «***Cloud Delivery***» : Packaging, vente et fourniture de services cloud

La première chaîne de valeur (1) est «classique» dans l'IT ; elle repose à la fois sur la valorisation des licences et des innovations ainsi que sur les capacités de mise en œuvre et d'infogérance. Elle est aussi novatrice de par les nouveaux modèles induits de fourniture de ressources. Différents modèles apparaissent avec le Cloud, essentiellement pour compenser le manque de maturité des infrastructures ou compétences clés : Cloud integrator, Cloud carrier. Leurs clients sont principalement les opérateurs de Cloud public ou les DSI mettant en œuvre un Cloud privé.
La fourniture de services cloud (2) constitue la seconde chaîne de valeur, délivrant la fourniture d'un service final d'infrastructures (IaaS), de plates-formes (PaaS), d'applications (SaaS) ou de processus métiers.

Enfin, la DSI amenée à renforcer ses rôles de gouvernance, audit et architecture dans le cadre de la définition et déploiement de services cloud, pourra se faire assister par des sociétés spécialisées à même d'appréhender les challenges technologiques et opérationnels de ces nouvelles offres : société de conseil et SSII.

### 4.1.1. L'évolution du positionnement des acteurs

- Positionnement «naturel», en continuité
  - Éditeur => Enabler/SaaS
  - Constructeur => Enabler/IaaS – Var
  - Intégrateur/SSII => Cloud integrator – Var
  - Cabinet de conseil => Business Process Cloud
  - Opérateur Télécom, Infogérant => IaaS, broker/Var

- Positionnement «complémentaire» : le Cloud et les nouveaux modèles économiques associés opèrent une transformation des acteurs, qui choisissent un positionnement multiple et parfois en complément ou compétition, par exemple :
  - Constructeurs => Cloud Integrator + Public SaaS en complément de l'offre (IaaS / PaaS), incluant la partie service et conseil (en compétition avec la fourniture de composants aux SSII et intégrateurs)
  - SSII allant vers le VAR : par exemple SSII revendant des abonnements Apps en compétition avec sa propre offre d'infogérance...

## 4.2. Impact pour les fournisseurs

La construction d'une offre de Cloud Computing impose des transformations significatives pour les fournisseurs.

### Des «contrôleurs» aux côtés de la DSI ?

**Côté client, eSCM réaffirme la légitimité de la DSI, porteuse d'un savoir-faire unique et seule capable :**

**1) De dialoguer et de challenger les prestataires**

**2) De traduire les besoins métiers en exigences fonctionnelles ou techniques**

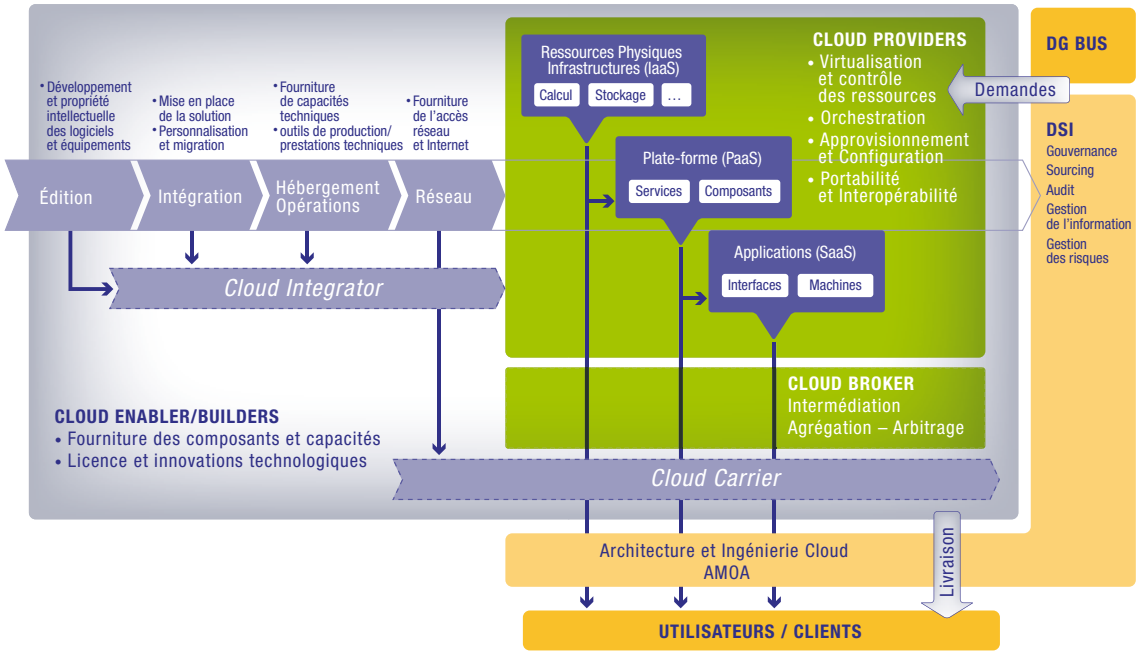
**3) De piloter efficacement les prestataires**

**4) De garantir la cohérence des SI internes, externalisés ou «cloudifiés».**

**À côté du client, un rôle de contrôle et d'audit spécialisé pourrait émerger, en interne ou via des acteurs indépendants, à la manière des bureaux de contrôle du bâtiment, qui ont un rôle légal ou prudentiel affirmé depuis des décennies.**

- **Fournisseurs d'IaaS :** pour un infogérant ou un hébergeur, cette transformation va consister dans l'adoption de nouvelles logiques :
  - Logiques de prestations par couche technique ou par compétence à un service de bout en bout, nécessitant une refonte des organisations ;
  - Logiques de « sur mesure » à un delivery model totalement industrialisé ;
  - Logique financière d'investissement financé par les clients à des investissements portés par le fournisseur.
- **Fournisseur de SaaS :** la transformation est encore plus profonde pour l'éditeur qui va devoir :
  - Changer de business model, passer d'un modèle « licence + maintenance » à un modèle où le coût est lissé sur plusieurs années, avec un revenu immédiat diminué, mais rendu beaucoup plus pérenne… tout en finançant d'autres investissements

## Évolution des chaînes de valeur




DR

- Développer un savoir-faire de gestion de services : supervision, gestion des demandes entrantes, help desk, gestion des incidents, production informatique (ou pilotage de son propre prestataire), gestion des changements…
- Revoir son cycle produit et se préoccuper de déploiements complexes : apprendre à faire évoluer une plate-forme multi-client / multi-versions / multi-paramétrages sans la casser, mettre en place des processus de livraison continue…
- Faire évoluer son produit pour faciliter son déploiement et son exploitabilité – voire parfois le réécrire pour en faire un produit massivement distribué et massivement multi-client.

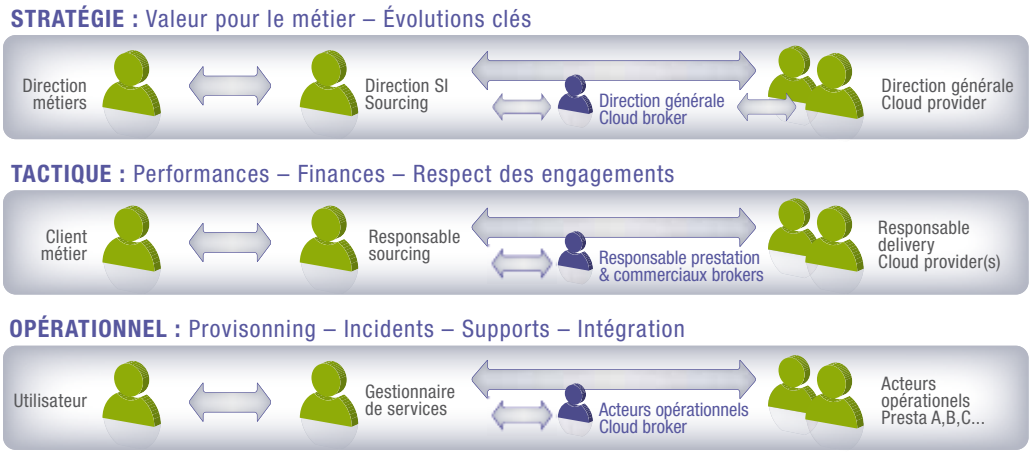
# 5. NOUVEAU RÔLE DE LA DSI

Une vision transversale est nécessaire pour :

- identifier les nouveaux rôles au sein de la DSI
- identifier les périmètres de responsabilité de chacun
- identifier les impacts sur l'organisation existante
- Accompagner les changements

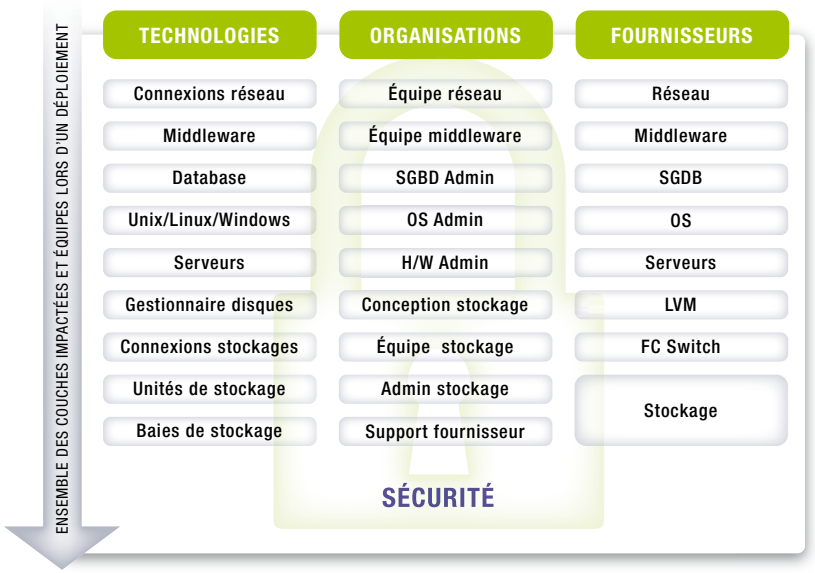
À l'exception des offres les plus standardisées de Cloud ou de SaaS publics, la plupart des contrats cloud continueront à nécessiter une

## Le pilotage du Cloud passe par des relations structurées




DR

## Le double défi technique et organisationnnel de la DSI




DR

relation forte entre les acteurs. Comme illustré dans le tableau ci-dessous, la nature de la relation et les sujets abordés vont évoluer : de la technique/opérationnel vers le résultat/l'alignement stratégique.

Dans les modèles de Cloud public, la relation va certes se déshumaniser… et encore ! Il est probable que de nombreuses offres seront portées par des intégrateurs/brokers de Cloud, qui offriront à leurs clients le même type de relation que celles apportées aujourd'hui par les intégrateurs de solutions techniques. De nouveaux médias relationnels émergeront également : forums, blogs, influenceurs…

Le client a souvent une vision d'acquisition par couche. Il cherche l'outil cloud qui pourra piloter son IT hétérogène existante. Comment garantir :

- La bonne intégration de l'ensemble des couches impliquées dans le service à délivrer,
- Leur automatisation,
- Leurs évolutions les unes par rapport aux autres dans le temps.

## 5.1. Pour le Cloud, de quelles compétences disposer ?

La DSI, si elle veut continuer à jouer son rôle, va devoir poursuivre et accélérer sa transformation, et renforcer ses compétences de gestion et de pilotage du portefeuille de services, via de nouvelles compétences/de nouveaux métiers :

- Service Management
- Vendor Management
- Conformité/Audit/Security Officer
- Architecte technique
- Product/Service line manager : compétence proche de celle existant aujourd'hui au sein des éditeurs de logiciels, c'est-à-dire chargée de :
  - Décider de la combinaison de services cloud à proposer aux utilisateurs.
  - Favoriser l'adoption et la réalisation de la valeur en soutenant les utilisateurs et en pilotant les déploiements, la conduite du changement.
  - Piloter l'évolution fonctionnelle des solutions et du mix de services.
  - Mener à bien l'analyse de la valeur « business » et « IT ».

Les rôles et responsabilités changent :

- **Côté IT :** se trouvent les responsables de la plate-forme «cloud». Il s'agit d'une équipe transverse qui maîtrise la couche de services fournis

- **Côté métiers :** dans le cas d'une plate-forme « as a service », les activités des équipes IT vont évoluer vers des rôles d'interfaces proactives entre les métiers et le fournisseur cloud.

### Pour le CRIP : « Le Cloud n'affaiblit pas la DSI : il la renforce »

**Avec le Cloud, les directions utilisateurs sont tentées d'acheter des services de leur côté, chacune y allant de sa solution miracle. Ce phénomène n'est pas sans rappeler l'arrivée du PC, devenu un temps synonyme pour la DSI de... perte de contrôle ! Et si cela se reproduisait aujourd'hui avec le Cloud – chacun dans son coin ?**

**Il faut dire que, vu de la place des utilisateurs, la DSI n'a pas que des avantages : *« elle filtre la relation avec les fournisseurs et ajoute systématiquement contraintes et délais supplémentaires »* entend-on régulièrement. Ainsi, on rapporte à titre d'anecdote que lorsque Derek Gottfrid a voulu traiter les 4 To d'archives du *New York Times* pour les héberger en ligne, il a fait appel au Cloud sans demander l'avis du service informatique du grand magazine. D'ailleurs, du fait de la transparence tarifaire qu'offre le Cloud, on peut s'attendre à ce que les directeurs généraux et financiers fassent pression sur les directeurs informatiques pour les inciter à passer en mode Cloud.**

**En réalité, c'est dans la construction du système d'information, son urbanisation, le lien du SI avec l'entreprise et son intégration que la DSI prend toute sa valeur ajoutée et sa légitimité. Le Cloud Computing renforce l'importance du rôle d'intégrateur de la DSI. Et ce rôle d'intégrateur Cloud de la DSI, n'est-ce point légitimement aux responsables infrastructure de s'en saisir ?**

Dans le contexte du Cloud, **certaines activités vont perdre de l'importance** et d'autres vont peser plus lourdement que par le passé, nécessitant pour le client et pour les fournisseurs le développement de capacités nouvelles.

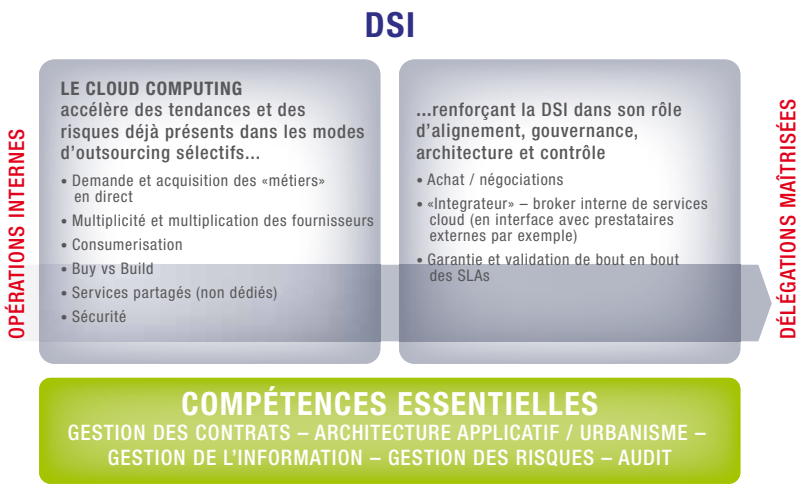
L'arrivée du Cloud confirme la convergence des compétences en matière d'exploitation et d'intégration. Là où subsistait une distinction entre profils « réseaux », « systèmes » et « stockage », les profils recherchés doivent pouvoir s'appuyer sur l'un de ces socles basiques de compétences et s'enrichir d'une seconde expertise. On recherche ainsi des « experts Data Center » qui paradoxalement ont tendance à devenir plus généralistes que les profils « classiques » d'administrateurs systèmes ou ingénieurs réseaux.

Le Cloud, avec sa complexité technique associée au mode service et à l'externalisation, amènera chaque collaborateur des équipes d'infrastructure et de production à développer des expertises avancées sur certains domaines techniques, tout en acquérant des compétences transverses sur la maîtrise économique et financière, la sécurité de l'information et les processus d'externalisation, y compris les achats.

Les filières éducatives doivent donc s'adapter en créant les formations ad hoc intégrant le volet réseaux, systèmes (incluant la virtualisation), infrastructure multi-technique, sans oublier d'y introduire un volet orienté performance et IT durable, aujourd'hui indissociable de toute fonction portant sur l'exploitation du data center.

L'adoption du Cloud Computing, et plus particulièrement dans un mode « interne », qui s'applique pour les entreprises et organisations d'une taille significative, impose le décloisonnement des équipes d'infrastructure et de production, traditionnellement organisées en « silos » (serveurs, stockage, réseaux, sécurité, etc.), afin de permettre la production de services IT selon des processus transverses, régis par les bonnes pratiques ITIL (Information Technology Infrastructure Library) et le référentiel eSCM (e-Sourcing Capability Model). Pour les entreprises ou organisations de taille plus limitée, l'adoption du Cloud demandera une certaine maîtrise des services externalisés.

Évolutions clés des compétences et des métiers




DR

## 5.2. Gouvernance, pilotage des prestations, exploitation quotidienne

Avec le Cloud, les aspects opérationnels étant plus que jamais sous contrôle du fournisseur, la gouvernance va devoir évoluer vers un pilotage par les engagements sur le service fourni, les risques et par la valeur créée.

Les nouvelles offres placent de plus en plus le prestataire comme un acteur majeur dans l'atteinte des objectifs de l'entreprise. Ainsi, le client ne sera plus seul décideur des solutions à mettre en œuvre. La gouvernance des fournisseurs de Cloud doit donc être structurée de sorte à assurer une interface représentative des besoins de l'entreprise et garante des résultats. Le Cloud induit un mode de fonctionnement nouveau entre la DSI et les directions métiers, et la nécessité pour la DSI d'intégrer et de maîtriser de nouveaux processus.

En effet, la possibilité offerte par le Cloud Computing aux utilisateurs d'accéder à des ressources informatiques à la demande exige de la part de la DSI :

- La maîtrise des capacités de ressources (capacités propres dans le cas du Cloud privé ; capacités des providers dans le cas du Cloud public) : t ressources sont ou seront disponibles pour les besoins des métiers ?
- La maîtrise de la demande globale des utilisateurs : quels sont ou seront les besoins des métiers ?

Si la DSI ne maîtrise pas les réponses à ces deux questions, le risque est grand d'une perte de contrôle, notamment dans le cas du SaaS où l'offre est directement disponible pour les utilisateurs.

La DSI doit donc aller vers une organisation de type industriel qui intègre :

- Un processus de gestion de la demande à court, moyen et long terme
- Un processus de gestion des capacités à court, moyen et long terme

## 5.3. Pilotage tactique et opérationnel, selon eSCM

Traditionnellement, dans le sourcing IT, le pilotage côté client est très orienté vers le contrôle des actions du fournisseur (normes techniques, méthodes opérationnelles...) ainsi que vers le pilotage des incidents, des performances et des coûts. eSCM propose un cadre de gouvernance plus complet reposant sur des activités opérationnelles, tactiques ou stratégiques, aligné avec ITIL et symétrique entre le client et le fournisseur. Dans le contexte du Cloud, certaines activités vont perdre de l'importance et d'autres vont peser plus lourdement que par le passé, nécessitant pour le client et pour les fournisseurs le développement de capacités nouvelles. Sans être exhaustifs, en voici quelques-unes :

### Évolution des métiers : plus d'analyse, moins d'exécution

**Les retours d'expérience partagés au sein du groupe de travail ad-hoc du CRIP incluent des projets opérationnels de Clouds «internes» très orientés «service», comme ceux déployés par une grande entreprise industrielle ou par une banque d'investissement, ainsi que des solutions de Clouds «externes», publics ou privés, comme les déploiements d'outils collaboratifs menés par deux grandes entreprises industrielles très internationales. Tous ces projets ont été initiés, ou à défaut pilotés, par les départements d'infrastructure et de production des entreprises concernées. Ils illustrent le fait que les tâches dévolues aux équipes d'infrastructure et de production s'appliqueront de plus en plus à des environnements dématérialisés, virtuels – par essence plus abstraits – et seront davantage portées sur l'analyse, l'expertise, le management, que sur l'exécution, la réaction et la répétition. Ainsi, ces métiers gagneront encore en intérêt et susciteront de nouvelles vocations auprès des jeunes diplômés.**

| | | Activité client | Activité fournisseur |
|---|---|---|---|
| Pilotage opérationnel | Activités techniques de fourniture du service. Contrôle des activités techniques | Forte baisse, du fait de l'industrialisation et de l'éloignement du provider (sauf Cloud privé). | Nécessité de disposer d'une capacité « service delivery » et « service support » sans faille. Un challenge pour les éditeurs basculant en mode SaaS |
| | Gestion des incidents et des problèmes | Perte significative de la capacité à influer sur la résolution des incidents et des problèmes récurrents face à un prestataire mutualisé. Le client va devoir développer une logique de gestion de disponibilité et de continuité. | Nécessité de fournir une lisibilité forte et une capacité de détection et de résolution d'incidents et de crises. |
| | Provisionnement, gestion des demandes | Une rigueur très forte devient nécessaire pour tracer et approuver les demandes de services, sous peine de perdre le contrôle des coûts et des usages. Autre nouveauté : disposer de processus permettant d'assurer le décommissionnement de services qui ne seraient plus nécessaires – faute de quoi le gain économique du Cloud risque d'être anéanti. | Capacité à provisionner et à tracer des unités d'œuvre très granulaires. |
| Processus tactiques | Gestion de la performance : respect des SLA | Les capacités à mesurer le service et les SLA doivent être renforcées, dans des contextes d'usage variable, multi-devices, globalisés. Par contre, les moyens d'action sont diminués (cas du Cloud public/communautaire) et non compensés par des pénalités peu efficaces. La performance va devoir être pilotée moins au quotidien, plus en amont et par des palliatifs – soit en gestion des risques. | Capacité à fournir un reporting détaillé sur les SLA |
| | Gestion financière | Un renforcement significatif des processus est à prévoir pour pouvoir gérer des demandes fluctuantes. | |
| | Gestion de la capacité | La gestion opérationnelle des capacités est assurée par le prestataire ; le client doit pouvoir se concentrer sur les capacités d'accès (notamment réseau) et sur l'anticipation/ prédiction de la demande. | Modèle d'ajout de capacité et maintien de l'évolutivité démontrable. |
| | Contrôle de la conformité | La capacité à auditer le prestataire devient clé. | |
| Activités stratégiques | Gestion de la demande | Le pilotage de la demande de services devient un processus clé. | |
| | Pilotage collaboratif, partenarial de la valeur | Le client va, plus que par le passé, devoir développer une capacité à établir et manager des relations partenariales et à piloter le Cloud par la valeur et les risques. | |
| | Pilotage stratégique | Le choix de recourir au Cloud doit intervenir au niveau stratégique de l'entreprise, certaines solutions telles que le SaaS pouvant avoir un impact structurant. | |

# 6. MÉTHODES, RÉFÉRENTIELS, NORMES, « STANDARDS » DU CLOUD

En matière de normes et de référentiels concernant l'informatique dans les nuages, il y a profusion d'initiatives et, sans doute possible, de bonnes volontés !

## 6.1. Où en sommes-nous aujourd'hui en matière de normalisation, de standardisation ?

Le battage médiatique autour du Cloud Computing a créé une certaine confusion, avec de nombreux efforts de standardisation et d'activités open source pas toujours cohérents. En voici un rapide aperçu.

- Le ***Cloud Standards Consumer Council*** doit permettre d'accélérer l'adoption des technologies de Cloud en pilotant les initiatives de standardisation dans l'intérêt des utilisateurs.
- Le ***Distributed Management Task Force*** (DMTF). Son Cloud Work Group a produit des use cases, des interfaces d'interopérabilité. Il a publié une « Cloud Service Broker interface » spécifiant la manière dont un « Cloud broker » peut recevoir et dispatcher des demandes de services répondant à des exigences de services données.
- Le DMTF publie les standards ***Virtualization Management*** (VMAN) ) qui incluent « l'Open Virtualization Format » largement supporté par les environnements de virtualisation. La version 1.1.0 est normalisée par l'ISO/IEC 17203. Il s'agit de standards de format des machines virtuelles (OVF) visant à garantir la compatibilité entre les différentes technologies de virtualisation (entre fournisseurs de Cloud et au sein des entreprises). Utilisé par un nombre croissant de produits du marché, c'est donc un format de conteneur très utile, qui continue à évoluer.
- Le ***European Telecommunication Standards Institute*** (ETSI) est l'initiateur d'un certain nombre de standards particulièrement pertinents pour l'industrie du Cloud Computing, et plus particulièrement les IaaS et les protocoles d'accès ou de communications internes, via son comité technique TC CLOUD (anciennement TC GRID).
- En ce qui concerne la terminologie, les travaux du ***National Institute for Standards and Technology***, (NIST) font figure de référence. Par ailleurs, son initiative SAJACLOUD (Standards Acceleration to Jumpstart Adoption of Cloud Computing) participe aux efforts de standardisation d'autres organisations.
- L'*Open Grid Forum* (OGF) développe un ensemble de standards dans le domaine de l'informatique distribuée.
- Le standard OCCI (***Open Cloud Computing Interface***) est un protocole et une API pour faciliter le développement d'outils interopérables pour la gestion des Clouds (intégration, portabilité, déploiement, montée en charge, supervision…). Initialement dédié

aux environnements IaaS, il est aujourd'hui également utilisable pour les environnements PaaS et SaaS.

- OASIS (***Organization for the Advancement of Structured Information Standards***) perçoit certains domaines du Cloud Computing comme une extension des modèles SOA (Service-Oriented Architecture) et de gestion du réseau. Ses membres sont engagés activement dans la construction de modèles du Cloud Computing en extension des standards existants, notamment en ce qui concerne les protocoles de management, la gestion d'identité, les formats d'échange de données, les annuaires et les modèles d'interopérabilité.
- Le TM Forum publie des référentiels de bonnes pratiques très utilisés dans le monde des opérateurs télécom. À ce titre, il a publié de nombreuses spécifications pertinentes pour les sujets de construction, management et interopérabilité du Cloud, notamment dans son « Integration Framework » : interfaces de management de services pour réseaux, interface de metering, de gestion d'identité, standards de développement d'un catalogue de services, etc.
- Une alliance étroite est née récemment entre le SNIA et le DMTF afin de bâtir un canal unique de communication pour ces deux organisations et de recevoir des uns et des autres les exigences, le design ainsi que le retour d'information sur les standards. Ces deux sociétés et d'autres organismes de standardisation (CSA « ***Cloud Security Alliance*** », OGF « ***Open Grid Forum*** », OCC « ***Open Cloud Consortium*** », etc.) coordonnent leurs efforts dans le groupement « ***Cloud Standards*** ».

Les travaux du monde libre sont également intéressants à suivre : openNebula, Reservoir, OpenStack, Compatible One sont autant d'implémentations concrètes de certains standards émergents (par exemple OCCI) qui, s'ils émergent comme standards de fait ouverts (à l'instar d'Apache pour http/html), peuvent faciliter l'interopérabilité à terme.

Cette liste est volontairement très incomplète. L'Open Networking Foundation, l'ISO, L'union internationale des télécommunications, l'IEEE (Institute of Electrical and Electronics Engineers), la FFII (Foundation for a Free Information Infrastructure) – et bien d'autres – ont toutes des initiatives, groupes de travail en cours ou en gestation pour développer leur propre vision d'un modèle de référence du Cloud et de normes plus ou moins généralistes ou spécialisées.

## 6.2. Standards de portabilité

« *Est-ce qu'une solution existe chez un autre fournisseur ou au sein même de l'entreprise pouvant reprendre l'ensemble de l'application qui aura été hébergée dans le Cloud ?* » ce point est fondamental à vérifier lorsque l'on contractualise avec un fournisseur de services Cloud, car il impacte fortement la capacité de réversibilité. Il ne s'agit pas d'une simple récupération des données brutes, il faut pouvoir les réinjecter dans une base de données standard puis exécuter toute la logique métier.

Sur un service d'Infrastructure, la réversibilité concerne les langages et interfaces de déploiement des ressources de type machines virtuelles (OVF), stockage et réseau. Sur un service de type plate-forme « as a Service », cela concerne les outils et langages de développements (Java conforme au standard Java EE, base de données SQL conforme au standard de l'entreprise, etc.). Et sur une offre Software as a Service, cela implique de prendre en compte la capacité de pouvoir disposer de l'offre logicielle permettant d'exécuter le service soit chez un autre fournisseur, soit chez soi.

La situation semble beaucoup moins avancée en ce qui concerne la garantie de portabilité d'un code applicatif, voire d'une application. En effet, si, à bas niveau, la standardisation autour de langages non propriétaires (Java, PHP…) et de frameworks ouverts (Spring, Eclipse) semble progresser doucement (voir les annonces récentes...) pour offrir une certaine garantie de pouvoir récupérer un code écrit dans le nuage (sur un PaaS), la réalité de la portabilité devient beaucoup plus complexe si l'on considère qu'un code est généralement optimisé pour le fonctionnement dans un environnement particulier (par exemple vis-à-vis d'une « Database as a service » particulière) et prendra souvent en compte également – et c'est nouveau – des adaptations non techniques, comme par exemple le fait de régler le code par rapport à la tarification du Cloud d'origine.

La portabilité du code est au moins aussi délicate et problématique en environnement Cloud qu'elle l'est, depuis des décennies, entre environnements traditionnels – même Unix, conçu au départ comme « non propriétaire et ouvert ». Le sujet est dominé par les fournisseurs, certains surfant sur la tendance en proposant des PaaS « portables » d'un environnement Cloud à un autre… En attendant l'émergence et l'adoption de standards éventuels (voir par exemple la jeune initiative du Cloud Data Governance Working Group de la Cloud Security Alliance), il appartient donc aux clients de s'armer de prudence et de faire des choix conscients !

**La portabilité du code** est au moins aussi délicate et problématique en environnement Cloud qu'elle l'est, depuis des décennies, entre environnements traditionnels.

## 6.3. Intégration avec le SI ; gestion du flux de données

L'intégration du Cloud avec le SI soulève notamment des problématiques d'architecture et de règles de sécurité. Une étude préalable doit être réalisée avant toute démarche d'intégration des deux systèmes. Elle devra établir les modes de communication, les règles de sécurité et les coûts engendrés par l'utilisation de modules Cloud par la plate-forme de la société. Par exemple, faire communiquer des données des systèmes locaux avec un ERP sur le Cloud nécessite de fixer le périmètre des données exposées, le volume (pour réduire l'utilisation des espaces temporaires de stockage), ainsi que la consommation du réseau de la plate-forme Cloud qui est souvent un module payant.

En fonction du type de service consommé et des choix associés (multi-locataires, dédié, public, privé), le niveau d'intégration et de sécurité associé peut varier : du simple utilisateur/mot de passe, en passant par une cryptographie des flux (SSL), au réseau privé virtuel (VPN) jusqu'au cryptage sur toute la chaîne (jusqu'aux données stockées).

Au-delà de la sécurité, il s'agit de traiter les points suivants :
- Transférer ses données
- S'assurer que les utilisateurs accèdent correctement aux services
- Gérer l'accès des utilisateurs aux données/services
- S'assurer de la cohérence des données entre applications
- Optimiser les processus métiers entre applications

Du point de vue applicatif ou système d'information (SaaS), l'intégration du Cloud avec le SI de l'entreprise est simultanément un sujet balisé (urbanisation et bonnes pratiques d'architecture telles que TOGAF) et un problème neuf et complexe. Dans le choix d'une solution SaaS, les critères d'interopérabilité avec le SI (interfaces standard vers des progiciels classiques, existence de web services, respect des éventuelles normes sémantiques existantes telles qu'EDI…) sont des critères de choix importants. Autres critères : la politique d'évolution fonctionnelle, le fait que ces évolutions s'imposent ou non au client (les « Season releases ») et le coût des interfaces (tarification au volume).

La DSI a un rôle évidemment critique sur ce point : si l'acquisition de solutions SaaS est préemptée par les métiers seuls, l'intégration et la cohérence avec le SI en seront compliquées. D'un point de vue technique, la situation est néanmoins facilitée par la disponibilité de protocoles ouverts et normés d'échanges comme les standards de l'OASIS Web Services Interoperability (WS-I).

À noter : certains acteurs se positionnent spécifiquement sur la fourniture de passerelles entre fournisseurs du Cloud, offrant (en mode SaaS évidemment) des interfaces points à points entre de nombreuses solutions cloud ou traditionnelles.

## 6.4. Interopérabilité entre différents Clouds

Aujourd'hui, l'interopérabilité entre différents Clouds au niveau le plus basique – la communication entre machines – est raisonnablement possible. Cela nécessite évidemment des travaux et l'établissement de standards appropriés pour l'interconnexion des réseaux, la fédération des identités, la gestion des accès et de la sécurité.

La portabilité et le management unifié (notamment, par exemple, le transfert automatisé de charges de travail ou de données) entre Clouds sont deux sujets plus délicats, pour lesquels des travaux de normalisation sont engagés (voir plus haut). Ce thème, à surveiller, devrait évoluer raisonnablement rapidement, sous l'impulsion de très grands donneurs d'ordres (dont le gouvernement américain ou l'Union européenne) et de certains éditeurs de briques cloud, qui ont tout intérêt à fournir ce type de portabilité.

L'Open Cloud Computing Interface (OCCI) est un ensemble de spécifications produit par l'Open Grid Forum, comprenant un protocole et une API ouverte permettant l'interaction avec des ressources hébergées sur les plates-formes de cloud d'une façon explicitement indépendante des fournisseurs, et pouvant être étendue afin de résoudre une gamme large de problématiques liées au Cloud Computing.

L'IEEE s'est également mise en mouvement et travaille sur un guide de portabilité et sur un standard d'interopérabilité et de fédération entre Clouds (« cloud to cloud »), définissant la topologie, les fonctions et la gouvernance permettant l'interopérabilité et la fédération de services.

L'Open Cloud Consortium vise à soutenir le développement de standards et de cadres d'interopérabilité entre les fournisseurs de services de cloud computing, mais aussi à développer des bancs de tests ainsi qu'à définir des implémentations de référence en open source. Il a notamment publié le MileStone Benchmark, qui cible plus particulièrement les hébergements de données sur les plates-formes de cloud computing de grande envergure.

## 6.5. Et le Cloud Storage ?

Le stockage des données est une composante essentielle dans le Cloud. Le « *Cloud Storage* » est confronté aux mêmes exigences que les autres services Cloud, c'est-à-dire : le paiement à l'usage, l'élasticité avec l'illusion de capacité à l'infini et la simplicité d'utilisation et de gestion. Il est donc important de standardiser la façon de gérer les différentes ressources que l'on peut proposer comme services de stockage ou services de donnée.

Outre OVF et OCCI déjà cités, le standard CDMI (Cloud Data Management Interface) du SNIA, apparu en 2010, définit une interface fonctionnelle que les applications peuvent utiliser pour créer, récupérer, mettre à jour et supprimer les données dans le Cloud. Concernant l'administration, CDMI permet de gérer les données, les conteneurs, les comptes utilisateurs, la sécurité des accès ainsi que la surveillance et la facturation.

## 6.6. Pour la sécurité, « Security-as-a-Service »

Différents groupes de travail sont constitués autour de la sécurité du Cloud. Le premier – ISO 27000 – fait référence en la matière, aussi bien pour ce qui est de l'informatique traditionnelle que dans le domaine spécifique du Cloud. Les autres sont le fruit d'initiatives diverses. En voici les principaux :

- ISO 27001/27002, norme internationale, très largem ent adoptée, de gestion de la sécurité de l'information.

- L'initiative ***Cloud Security Alliance*** regroupe de nombreux acteurs du Cloud Computing avec pour objet d'éditer un ensemble de documents portant sur ce thème. Leur « ***Security Guidance for Critical Areas of Focus in Cloud Computing*** », dont la 3ème

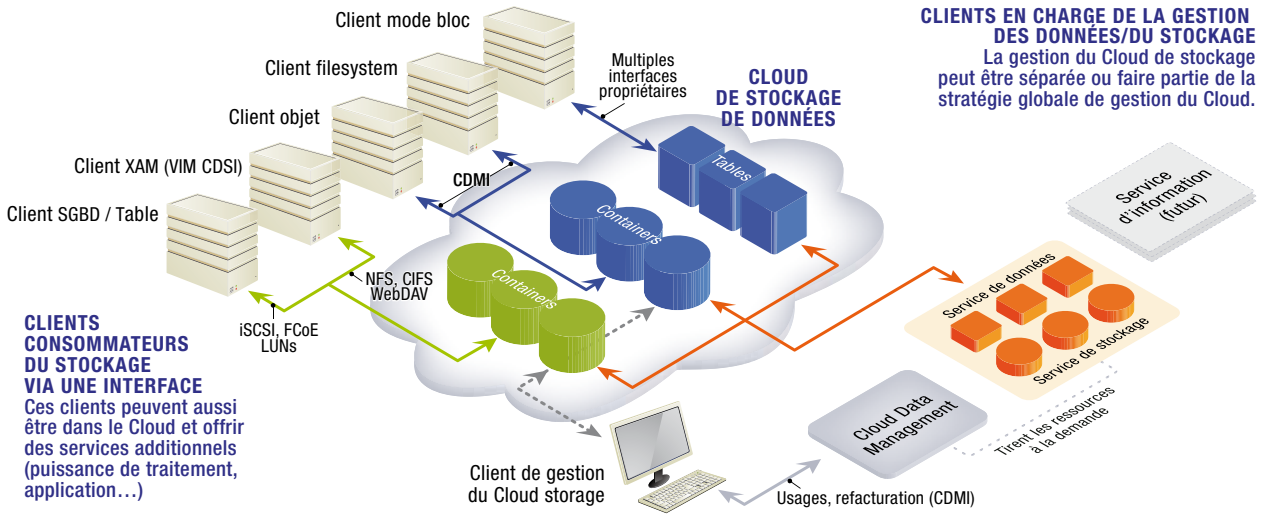
édition a été publiée à la mi-novembre 2011, compile un ensemble complet et structuré de bonnes pratiques en matière de sécurité des plates-formes Cloud. Trois grands thèmes sont abordés – architecture, gouvernance, opérations – et quatorze domaines sont identifiés, allant du cadre architectural du Cloud jusqu'au concept de « Security-as-a-Service ». Pour chacun de ces domaines sont listées des recommandations et des exigences. Ce document est plutôt exhaustif, puisqu'il visite un grand nombre de domaines de la sécurité informatique, physique comme logique. Reste à voir comment, en pratique, l'implémentation de ces pratiques peut être vérifiée et mesurée par les entreprises clientes, utilisatrices du Cloud Computing.

- La « ***Cloud Controls Matrix*** » est plus spécifiquement conçue pour fournir les principes de sécurité fondamentaux qui doivent guider les fournisseurs de services Cloud et assister les acheteurs dans leur évaluation des risques.

- Le « ***Top Threats to Cloud Computing*** » est un rapport qui a pour objectif de fournir des éléments aux entreprises pour les aider à bien gérer le risque en matière de stratégie d'adoption du Cloud.

- « ***CloudAudit*** » doit fournir une interface commune et un espace de nommage permettant aux fournisseurs de service cloud d'automatiser l'audit, l'affirmation, l'évaluation et l'assurance (automated audit, assertion, assessment, assurance) de leurs environnements d'infrastructure (IaaS), de plate-forme (PaaS) et d'applications (SaaS) et de permettre à des clients autorisés de faire de même, via une interface et une méthodologie ouvertes, sûres et extensibles.

## Évolutions clefs des compétences et des métiers




DR

- Le « ***Cloud Trust Protocol*** » disponible dans sa seconde version est un protocole d'échange d'informations de transparence sur le Cloud permettant de répondre à des questions telles que : où sont mes services ? Qui y a accès ? Quelle est leur configuration technique ?

## 6.7. Pour la gouvernance ; la conformité réglementaire

Version « Standard International » de SAS 70 dont elle se veut l'héritière, ISAE 3402, publiée en juin 2011 par l'IAASB (, a pour objectif d'évaluer la capacité d'un fournisseur externe à fournir un niveau de qualité de service, de risque et de sécurité compatible avec les exigences et les devoirs de son client – notamment en regard des responsabilités légales de ce dernier envers les réglementations comptables type Sarbane-Oxley. Il prévoit deux types de rapports (déclaratif et évaluation testée).

## **Cloud et Sécurité :** les questions du CRIP

**Dans sa première enquête sur le Cloud, effectuée auprès de ses adhérents en 2010, les préoccupations liées à la sécurité dominaient les questionnements sur l'adoption de modèles Cloud. En 2011, le groupe de travail « Cloud » a initié un travail de fond avec des RSSI (Responsables de la Sécurité des Systèmes d'Information) d'entreprises et entités publiques sur ce thème, tout en créant ainsi le « Cercle des RSSI» du CRIP. Des premiers échanges initiés, il ressort certains points marquants, souvent exprimés sous forme de questions à se poser :**

**La sécurité (de l'information) est l'affaire de tous dans l'entreprise, à tel point qu'il est constaté que, d'eux-mêmes, les acteurs métier s'inquiètent de la sécurité autant que les responsables infrastructure et production informatique.**

- **« Passer sur le Cloud» pose le difficile problème de la qualification des données, et même des processus. Comme définir ce qui est confidentiel et ce qui ne l'est pas ?**
- **L'enjeu avec les données n'est pas tant leur isolement, leur protection, mais bien plus leur sélection avant de leur appliquer des politiques et traitements ad-hoc.**
- **Il convient avant tout de classifier les données, ce qui est de la responsabilité des métiers, pas des RSSI.**
- **L'adoption de modèles cloud impose de passer progressivement d'un modèle de sécurité « périmétrique» à un modèle de « sécurisation de la donnée». Mais si une application d'âge significatif n'a pas été prévue pour gérer les accès dans ce mode-là, et sur laquelle il n'est pas prévu de faire de nouveaux développements, comment l'adapter à ce nouveau modèle de sécurité ?**
- **Il est convenu que, même s'il complique les opérations, le chiffrement est la seule solution de confidentialité qui soit efficace pour protéger les données hébergées dans un Cloud.**
- **La sécurité ne se juge pas seulement en terme de confidentialité des données, mais également dans leur disponibilité : 80 % des incidents de sécurité viennent en fait d'incidents de disponibilité.**
- **Enfin, il convient d'être attentif aux clauses dans les contrats des fournisseurs de services Cloud qui, très souvent, affirment « *nous ne gérons ni votre disponibilité ni votre confidentialité, c'est à vous de trouver des solutions pour le faire*».**

# POUR EN SAVOIR PLUS

**Sources et documents utiles :**

- Syntec Numérique : « Livre blanc du Cloud Computing » et « Livre blanc Sécurité du Cloud Computing » : www.syntec-numerique.fr
- Sur le référentiel eSCM : www.ae-scm.fr
- Sur le CRIP : www.crip-asso.fr et www.itiforums.com
- http://fr.wikipedia.org/wiki/Open_Virtual_Machine_Format
- http://www.snia.org/cdmi
- http://occi-wg.org/
- http://Cloud-standards.org
- http://www.dtmf.org/standards
- http://www.ogf.org/public_comment_docs/

# LES RÉDACTEURS DU LIVRE BLANC

### Rédaction du Livre Blanc

- *Rédaction et rewriting :* **Philippe Grange** – Faits et Chiffres
- *Chef de projet :* **Céline Ferreira** – ITS Integra
- *Délégué Métiers :* **Éric Lerouge** – Syntec Numérique

### Ont contribué à l'élaboration du Livre Blanc :

- Éric Bezille – Oracle
- Rachid Boularas – NetApp France
- Renaud Brosse – Ae-SCM
- Fabien Butel – Oracle
- Sébastien Darde – Intercloud
- Jérôme Dilouya – Intercloud
- Séverine Duhau – VeePee
- Zarah Essi – Spie Communications
- Julien Lesaicherre – Microsoft France
- Yannick Ragonneau – Dell
- Serge Robert – Open Groupe
- François Stephan – CRIP
- Cyril Van Agt – NetApp France

### Ont également contribué au Livre Blanc :

- Olivia Flipo – OF Avocat
- Marie–Noëlle Gibon – Ae-SCM
- Franck Guy – Ae-SCM
- Patrick Joubert – CRIP
- Mourad Kacir – Ae-SCM
- Nicolas Koleilat – Sopra Group
- Geoffroy de Lavenne – ITS Integra
- Mahasti Razavi – August & Debouzy

### Remerciements

Nous tenons à remercier tous les membres du Comité Infrastructure et Services de Syntec Numérique.

Syntec NUMERIQUE | DES ENTREPRISES QUI CHANGENT LE MONDE

3, rue Léon Bonnat / 75016 Paris / Tél. 01 44 30 49 00 / Fax. 01 42 88 26 84
www.syntec-numerique.fr / www.passinformatique.com