cigref
Réseau
de Grandes Entreprises

PROMOUVOIR LA CULTURE NUMERIQUE

COMME SOURCE D'INNOVATION ET DE PERFORMANCE

Fondamentaux du Cloud Computing

Le point de vue des Grandes Entreprises

Mars 2013

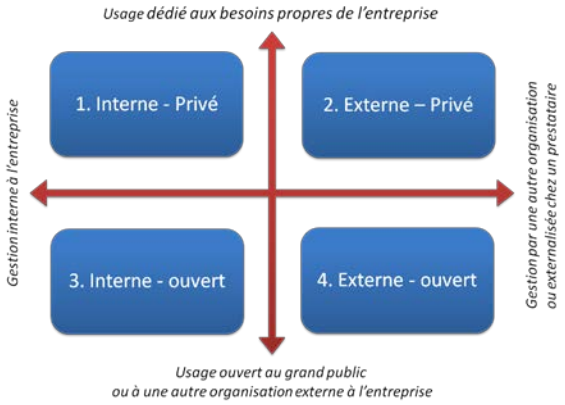
SYNTHÈSE

Les travaux passés du CIGREF avaient révélé plusieurs éléments de tension dans la compréhension du *SaaS* et du *Cloud Computing*. Le premier d'entre eux était l'absence d'une définition claire de ces concepts. Le groupe de travail du CIGREF s'est donc intéressé cette année aux fondamentaux du *Cloud Computing*. Il les a revisités et redéfinis en fonction de la compréhension et de sa mise en œuvre dans les entreprises et non à partir des offres du marché de l'écosystème IT.

Le groupe de travail a identifié quatre points qui permettent de définir un *Cloud* :

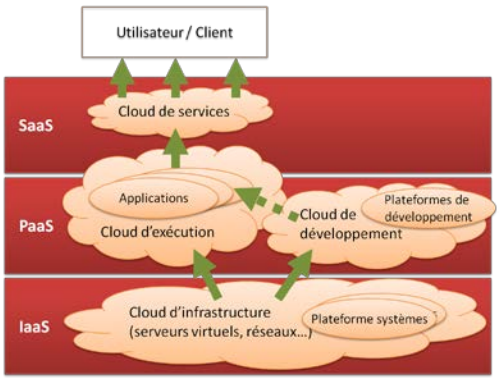
1. Un *Cloud* est toujours un espace virtuel,
2. contenant des informations qui sont fragmentées,
3. dont les fragments sont toujours dupliqués et répartis (ou distribués) dans cet espace virtuel, lequel peut être sur un ou plusieurs supports physiques,
4. qui possède une « console (ou programme) de restitution » permettant de reconstituer l'information.

Le groupe de travail a aussi décrit et détaillé quatre typologies de *Cloud Computing*, que l'on peut trouver dans les organisations membres du CIGREF. Chacune d'entre elles a été définie et mise en regard du modèle de service (*SaaS*, *Paas*, *Iaas*).



Source CIGREF

Au cours des échanges et des partages d'expérience, de nombreux conseils et bonnes pratiques ont été formulés. Le groupe a rassemblé ces informations et les a organisées en fonction des quatre typologies de *Cloud* définies. Fournissant ainsi une liste de points d'attention pour toute entreprise s'intéressant au *Cloud Computing*.



Source CIGREF

Le CIGREF, Réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de « …*promouvoir la culture numérique comme source d'innovation et de performance*… »

Titre du rapport : *Fondamentaux du Cloud computing* - Le point de vue des grandes entreprises

Equipe du CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directeur de mission
Anne-Sophie BOISARD – Directeur de mission
Josette WATRINEL – Secrétaire de direction
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

Remerciements :

Nos remerciements vont à Gérard RUSSEIL, DSI de CHOREGIE, qui a piloté cette réflexion.

Nous remercions également les membres du groupe de travail, qui ont participé à cette étude :

Michel BENARD - GROUPEMENT DES MOUSQUETAIRES - INTERMARCHÉ	Arnaud LE CONTE - GROUPEMENT DES MOUSQUETAIRES - INTERMARCHÉ
Cyril BARTOLO - LAGARDÈRE	Philippe LEBAS - ELIOR
Éric BARNIER - AÉROPORTS DE PARIS	Mina LEJAMBLE - AGIRC ARRCO
Laurent BIEBER - SNCF	Guillaume LIBET - CNES
Thierry CHAMPEROUX - MAIF	Christel LOITRON - OCP - GEHIS
Jean-Yves CHOURAQUI - L ORÉAL	Annelise MASSIERA - DISIC
Cédric SIBEN - MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DU COMMERCE EXTÉRIEUR	Marc MEYER - MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DU COMMERCE EXTÉRIEUR
Léon DE SAHB - STEF	Hélène MONIN - MANPOWER
Luc DEBRAY - AGIRC ARRCO	Alain MOUSTARD - BOUYGUES TELECOM
André DELEVAQUE - NEXTER GROUP	Bernard PARMENTIER - AIR LIQUIDE
Jean-Pierre DELHEAU - RTE	Jean-Luc PAULIN - AMADEUS
Jean-Yves DROUGLAZET - MAIF	Alain PERONNET - RENAULT
Bernard DUVERNEUIL - ESSILOR	Jean-Luc RAFFAELLI - LA POSTE
Marie-Hélène FAGARD - EUROPCAR	Claude ROUCHE - SAUR
Jean-Louis GHIGLIONE - RENAULT	Thierry SABLE - TOTAL
Stéphane HUIGNARD - LACTALIS	Caroline SANDLER-ROSENTAL - CLUB MÉDITERRANÉE
Hervé JEGO - GENERALI	Pierre DE LAJARTE - RÉSEAU FERRÉ DE FRANCE
Sylvie LABETOULLE - GEODIS	Grégory SILVAIN - EURO DISNEY
Régis LACOUR - INSERM	Pierre TOMIAK - CNES
Gérard LAGO - RTE	Christian VALIN - LACTALIS
Hervé LAMBERT - GENERALI	André-Gilles VITTEK - EDF

Publications CIGREF en lien avec ce rapport :

2013 - *Cloud* et protection des données : guide pratique à l'attention des directions opérationnelles et générales
2012 - Quelle politique d'infrastructure de l'entreprise numérique ?
2011 - La compréhension du *SaaS* par les grandes entreprises
2010 - Position du CIGREF sur le *Cloud Computing*
2010 - Impact du *Cloud computing* sur la fonction SI et son écosystème
2010 - Les dossiers du Club Achats – *Cloud Computing*

Pour tout renseignement concernant ce rapport, vous pouvez contacter le CIGREF aux coordonnées ci-dessous :

CIGREF, Réseau de Grandes entreprises - 21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00 Courriel : contact@cigref.fr Site internet : http://www.cigref.fr/

SOMMAIRE

FIGURES

INTRODUCTION

Depuis maintenant 3 ans, le CIGREF s'intéresse au *Cloud Computing*[1] et aux modèles de service.

Déjà en 2010, l'offre de *Cloud Computing* faisait partie du paysage des solutions et services liés au SI. Le CIGREF le définissait alors comme une **nouvelle manière pour les entreprises d'acheter et de consommer des services liés aux SI dans le monde au travers du réseau internet**. A l'époque on parlait néanmoins plus de *SaaS*[2] parce que le marché était en cours de structuration.

L'offre répondait bien à certains besoins (applications transverses), moins à d'autres (aspects transactionnels et ERP notamment) et était plutôt perçue comme **une solution à combiner aux solutions existantes**. Mutualisation des ressources, paiement à l'usage, modularité et standardisation des fonctions proposées étaient les principales caractéristiques identifiées.

Les travaux des groupes de travail CIGREF, en 2010[3] et 2011[4], sur le *Cloud*[5] et le *SaaS* avaient néanmoins permis de souligner plusieurs **éléments de tensions dans la perception du *SaaS* entre les entreprises utilisatrices et l'écosystème IT**.
Les échanges avaient notamment montré le décalage de posture entre les fournisseurs et les entreprises utilisatrices, notamment sur l'interopérabilité des solutions et la réversibilité des données.

Les échanges avaient aussi démontré **les potentiels du *SaaS* et du *Cloud Computing* vis-à-vis des processus d'innovation** : flexibilité des solutions, rapidité de déploiement, investissement moindre à court-terme. Ils avaient également souligné le **besoin d'un accompagnement des métiers par la DSI dans l'acquisition de solutions *SaaS***.

---

[1] L'expression française pour *Cloud Computing* est « Informatique en nuage ».

[2] *SaaS* : *Software as a Service* (logiciel à la demande)

[3] « Position du CIGREF sur le *Cloud Computing* » : http://www.cigref.fr/position-du-cigref-sur-le-cloud-computing
« Impact du *Cloud computing* sur la fonction SI et son écosystème » : http://www.cigref.fr/impact-du-cloud-computing-sur-la-fonction-si-et-son-ecosysteme

[4] « La compréhension du *SaaS* par les grandes entreprises » : http://www.cigref.fr/la-comprehension-du-saas-par-les-grandes-entreprises

[5] On utilisera indistinctement dans ce document le mot *Cloud* lorsque l'on parlera d'un projet de *Cloud Computing* ou du *Cloud* en tant qu'outil. Cette expression sera aussi utilisée lorsque l'on parlera des modèles (technologiques, économiques) que le concept véhicule.

Aujourd'hui certains éléments se sont précisés :

- Le *Saas* est perçu comme un excellent moyen de **servir les directions métiers sur leur besoin en applications** et de **leur offrir**, par là-même, **des services et applications innovants.**

- C'est aussi un moyen de **répondre à un besoin de flexibilité** en adaptant très rapidement les infrastructures ou architectures à des **besoins ponctuels mais variables.**

- Le *SaaS* peut permettre de **diminuer les coûts de développement et d'intégration** des applications métiers. Mais l'offre est encore faible et les solutions en mode de service sont à ce jour relativement spécifiques et autonomes : **il y a encore peu d'intégration possible.**

- Dans sa définition de 2010, le CIGREF indiquait : « Quelle que soit la formule retenue par l'entreprise cliente, l'originalité du *Cloud computing* réside dans son modèle de facturation à l'usage, donc dans sa lisibilité, sa variabilité et sa prédictibilité des coûts ». Aujourd'hui, **la prédictibilité des coûts n'est pas garantie à plus de 2 ou 3 ans**. **Le *Cloud Computing* garantit par contre la « plasticité » des solutions**, par exemple, en cas de changement de volumes.

- **La notion de consommation prévaut sur la notion d'usage** : on achète un abonnement, un permis de consommer, on n'achète pas une licence d'utilisation. Le *SaaS* propose donc la possibilité de **passer d'une logique budgétaire d'investissement à une logique de fonctionnement**, se traduisant par la diminution des coûts d'acquisition et de maintenance.

- Alors qu'avant les utilisateurs n'avaient pas conscience de ce qui était mis en place et consommé, le *Cloud Computing* permet aussi **d'apporter et de valoriser une vision immédiate de la consommation financière à l'usage**.

- Les **applications *SaaS***, offrent une **standardisation fonctionnelle** (les mêmes services applicatifs sont disponibles pour tous les utilisateurs, sans développement particulier) alors que les **applications traditionnelles sont spécifiques** et souvent adaptées à l'usage d'une ou de plusieurs populations ciblées.

- La forte disparité économique entre les fournisseurs rend les comparaisons difficiles. Les modèles (économiques ?) ne sont pas encore bien établis et standardisés et **il est donc difficile de mesurer les TCO[6] possibles des différentes offres.**

[6] TCO : *Total Cost of Ownership* (Coût total de possession)

- Dans le cas d'un *Cloud*, les solutions techniques des fournisseurs ne suffisent pas : les entreprises clientes **doivent aussi avoir les compétences et les ressources en interne** pour le paramétrer au mieux de son usage (de la même façon que pour les ERP au début des années 2000). Un **nouveau métier** est peut-être en train d'apparaitre : paramétreur de *Cloud* (comme il existe paramétreur ERP).

Les offres ont donc évolué, les usages et les concepts se sont précisés. Mais il est apparu au fil des échanges qu'**il n'y a pas véritablement de compréhension commune**, chacun donnant sa définition du *SaaS*, *PaaS*[7], *IaaS*[8], et du *Cloud*, **définitions qui, du reste, varient dans le temps**.

Au cours des réunions de travail, le CIGREF a donc souhaité mettre en commun la connaissance et l'expérience que ses entreprises membres ont du *Cloud Computing*, pour **décrire de manière représentative leur réalité des projets *Cloud* et l'usage qu'elles en font**.

REVISITONS LA DÉFINITION D'UN *CLOUD*

Toutes les entreprises présentes dans le groupe de travail du CIGREF **ont un projet de *Cloud Computing* en cours.** Certaines ont même déjà mis en œuvre leur propre *Cloud* en interne. Elles savent donc pour la plupart ce qu'est un *Cloud*. Malgré tout, au cours des différentes discussions, il est rapidement apparu que le concept de « *Cloud Computing* » peut être expliqué avec des **définitions différentes, et qui évoluent différemment en fonction des acteurs qui l'emploient**. Les entreprises utilisatrices comme celles de l'écosystème IT usent de termes plus en lien avec leur propre stratégie *business* que dans un esprit de clarification.

Le groupe de travail a donc souhaité, pour **parler d'une même voix et avoir une compréhension commune**, travailler dans un premier temps sur une définition partagée du *Cloud Computing*.

Cette définition repose sur quelques constats simples :

- Un *Cloud* est au départ une **solution technologique,** mais sa définition dépend avant tout de **l'usage qu'on en fait**. On pourra trouver des *Clouds* de services qui offrent des solutions applicatives qui concernent directement les utilisateurs finaux, comme des *Clouds* d'infrastructures qui concernent les centres de production et d'exploitation, en traitant plus de la virtualisation nécessaire pour offrir des infrastructures de serveurs ou réseaux.

[7] *PaaS* : *Plateform as a Service*
[8] *IaaS* : *Infrastructure as a Service*

- Si **l'accès** à un *Cloud* se fait toujours par **un modèle de service**[9], l'inverse n'est pas vrai. En effet de nombreuses applications « *as a Service* » ne sont pas des *Clouds* : ce sont de simples applications « classiques » qui s'appuient sur une infrastructure traditionnelle de serveurs web, serveurs de GED ou sur un ERP. Encore maintenant la confusion est entretenue par de nombreux acteurs pour des raisons de marketing.

- Le modèle du *Cloud Computing* **est capable de traiter indifféremment** les trois couches communément utilisées du modèle de service :
  - Le ***IaaS*** : *Infratructure as a Service*
  - Le ***PaaS*** : *Plateform as a Service*
  - Le ***SaaS*** : *Software as a Service*

  C'est la force du *Cloud Computing* : il peut soit traverser l'ensemble de ces couches, soit avoir un comportement spécifique à chacune d'entre elles.

Pour le groupe de travail du CIGREF, même si cela peut paraitre basique, un *Cloud* est avant tout **une solution de stockage d'informations**[10] (au sens large du terme : données structurées ou non, logiciels, images, etc.) sur une ou plusieurs machines qui n'ont pas **d'attribution fonctionnelle particulière : elles peuvent se substituer les unes aux autres**.

Un *Cloud* **se concentre sur la donnée**[11] **indépendamment du support,** et **est capable de la restituer indépendamment de sa localisation**.

Dans sa recherche d'une définition, le groupe de travail a identifié **quatre points** qui permettent de caractériser un *Cloud* :

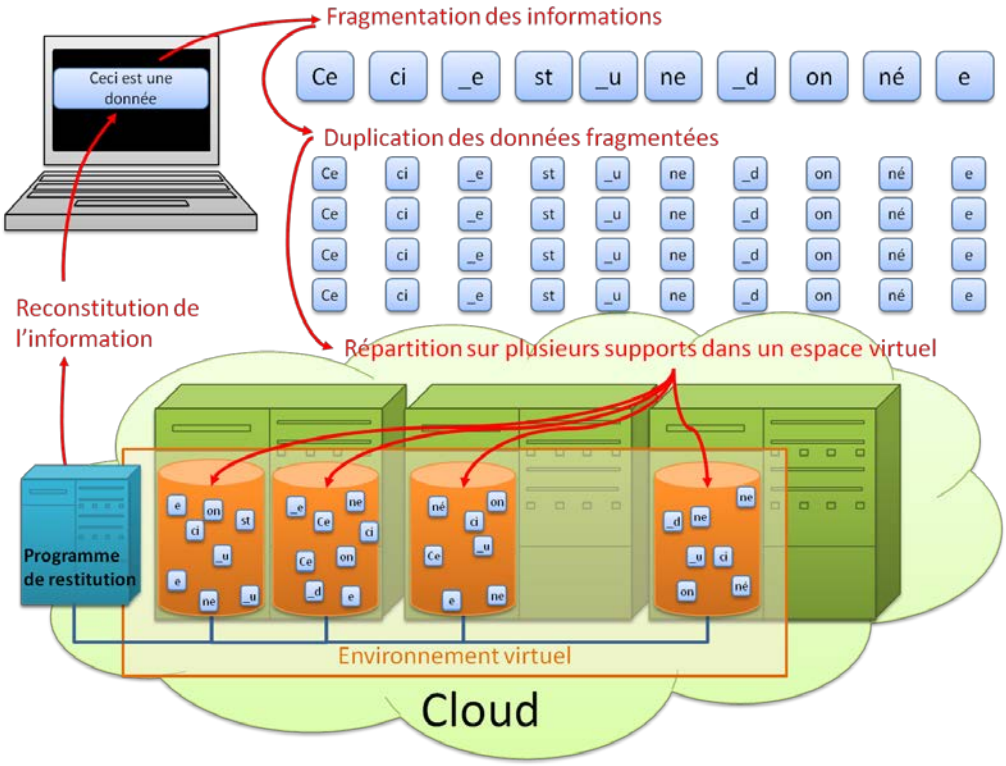
- Point 1 : Un *Cloud* est toujours **un espace virtuel,**
- Point 2 : Un *Cloud* contient des **données** qui sont **fragmentées,**
- Point 3 : Les **fragments de données** d'un *Cloud* sont toujours **dupliqués** et **répartis** (ou distribués) dans cet espace virtuel, lequel peut être **sur un ou plusieurs supports physiques**,
- Point 4 : Un *Cloud* possède une « **fonction de restitution** » permettant de **reconstituer les données**. Cette fonction peut être intégrée à la gestion du *Cloud* ou déportée sur l'application qui fournit le service.

[9] Un modèle de service permet d'externaliser intégralement un élément (fonction ou application) du système d'information d'une organisation et de l'assimiler à un coût de fonctionnement plutôt qu'à un investissement. On parle alors d'un élément « *as a service* ».

[10] Une « information » est un élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué (Larousse).

[11] Une « donnée » est la représentation conventionnelle d'une information en vue de son traitement informatique. Un ensemble de données constitue une information pouvant être conservée ou communiquée (Larousse).

Si l'une de ces quatre conditions n'est pas établie, nous ne sommes pas en présence d'un *Cloud*



(Source CIGREF 2013)

Figure 1 : Les 4 points permettant d'identifier un *Cloud*

En plus de ces points indispensables, il ressort également de ces travaux :

- Qu'**il n'est pas possible de savoir où se trouve une information particulière** (d'où la notion de « *Cloud*/nuage »). En effet, les fragments des données la constituant sont répartis sur l'ensemble des supports/*devices* composant le *Cloud*, et seule une « application de restitution » peut les localiser pour reconstituer les données et fournir une information complète.
  Cette faculté de distribuer des données permet d'étendre un *Cloud* à plusieurs *datacenters* disposés dans des lieux géographiquement éloignés et reliés par des réseaux hauts débits. Mais de nombreuses offres de *Cloud* se limitent à une répartition sur un ensemble de serveurs dans un unique *datacenter*.

- Que **la granularité de la fragmentation est importante**.
  - En effet, si les **fragments sont trop signifiants**, il sera possible d'en **lire le contenu**, mais aussi les **traitements - pour une plus grande fragmentation - seront donc plus nombreux**.

- Si les fragments sont **trop petits (au-delà du nécessaire sécuritaire)**, ce sera le **nombre d'accès** nécessaires pour reconstituer les données d'une information qui pourra être pénalisant en termes de performances.

En tout état de cause, **la fragmentation des données augmente la fiabilité et la sécurité mais peut ralentir leur agrégation**. Dans ce cas, la qualité du réseau est importante, notamment dans le cas d'un *Cloud* qui s'appuie sur plusieurs *datacenters* reliés entre eux.

- Que **la reconstitution des données** pour la délivrance d'une information, l'exécution d'une application ou l'accès à une fonction **constitue le « service » fourni**.

- Que **cette définition peut s'appliquer de manière identique quel que soit le modèle de service** mis en œuvre : *IaaS*, *PaaS* ou *SaaS*.

En termes de mise en œuvre, d'infrastructure et de sécurité, il est alors de possible de déduire plusieurs éléments importants issus des quatre points cités précédemment :

- **La perte** d'une partie d'un *Cloud* (une machine par exemple) **n'a pas d'effet sur les informations** puisqu'elles sont dupliquées et réparties sur plusieurs machines ou sur plusieurs sites. Une donnée est donc stockée en de multiples endroits. Dans ce cas, la sauvegarde des serveurs d'un *Cloud* est-elle toujours nécessaire ?

- De même, si un *Cloud* venait à manquer de ressources dans les serveurs existants, **il est alors possible d'ajouter des *devices*[12]** supplémentaires. Un *Cloud* s'adapte alors naturellement à la volumétrie nécessaire, **il est dimensionnable**. Cette particularité permet notamment d'utiliser de manière optimum l'espace disponible : dans un *Cloud* les données « remplissent » la place disponible plutôt que d'être « assignées » à des espaces déterminés. Certains membres du CIGREF, en passant de *datacenters* classiques à un *Cloud,* ont diminué considérablement le nombre de serveurs mis en œuvre.

- De la même façon, **le vol (ou la délivrance) des données d'un serveur** ou d'un ensemble de serveurs **ne permet pas de lire les informations** s'y trouvant stockées puisque chacune d'elles ne contient que des fragments de données. Seul le programme de reconstitution des informations (« la console de restitution ») est capable de faire le lien entre les fragments. Si en plus les données ont été cryptées (avec une clé RSA par exemple) avant d'être fragmentées, la lecture des fragments en direct devient quasi impossible. Ce point particulier dépend néanmoins du niveau de

[12] Essentiellement des serveurs, mais il est possible d'imaginer dans l'absolu d'utiliser les espaces de disque disponibles sur n'importe quelle machine (serveurs, *desktop*, *laptop* etc.) raccordée à un réseau.

fragmentation des données, des gros fragments seront plus signifiants et permettront de lire plus d'information.

- En termes de protection et de sécurité, **l'élément critique** n'est donc pas le *Cloud* en lui-même avec ses serveurs de données, mais **« l'application (ou console) de restitution** » qui permet de reconstituer les données nécessaires à la délivrance du service. **C'est elle qu'il faut protéger**. Il faut notamment se soucier de son emplacement géographique et de quelle législation elle dépend (par exemple dans le cadre du *Cloud* d'un prestataire).

PROJECTION SUR LES MODÈLES DE SERVICES

Le *Cloud Computing* est donc une solution qui fournit un espace dans lequel il est possible de placer, de manière virtuelle, des infrastructures serveur ou réseau, des plateformes de développement ou d'exécution, des catalogues de service etc. Un *Cloud* est ainsi capable **de traiter les différentes couches du modèle « *as a service* »**, de l'infrastructure jusqu'à l'utilisateur.

CLOUD & IAAS - INFRASTRUCTURE AS A SERVICE

Il ne faut pas confondre une infrastructure *Cloud* et un *Cloud* d'infrastructure :

- une infrastructure *Cloud* correspond à l'ensemble des ressources logicielles et matérielles qui sont nécessaires à **la constitution du *Cloud***. Cette infrastructure est particulièrement nécessaire lorsqu'une entreprise met en place son propre *Cloud* en interne
- un *Cloud* d'infrastructure est **le service rendu par le *Cloud*** : une infrastructure virtuelle sur laquelle il est possible de bâtir une solution applicative par exemple. C'est ce qui est fourni à une entreprise dans le cas d'un *Cloud* d'infrastructure externe.

Le *IaaS* concerne essentiellement **les *Clouds* d'infrastructure**.

Ces derniers fournissent à la demande un ensemble de services de niveau « bas », c'est à dire des serveurs, réseaux etc. Cela permet ainsi à une entreprise cliente de pouvoir **bénéficier de la puissance d'une infrastructure, ponctuellement, sans devoir investir beaucoup**.

Lorsqu'il y a une **certitude de variations fortes de charge**, ou une **incertitude sur la capacité d'une infrastructure à délivrer un service**, le *Cloud Computing* est alors une solution très adaptée : par exemple pour des besoins de type paie, messagerie ou éditique (création

massive et ponctuelle de documents). De plus le *Cloud* peut permettre de tirer parti au maximum du partage du matériel (processeurs, disques etc.).

Dans un *Cloud* d'infrastructure, l'utilisateur, ou l'entreprise cliente, est maître de son environnement virtuel et peut y installer ce que bon lui semble. De nombreuses offres proposent, par exemple, l'installation de serveurs virtuels, configurables à la demande, sur lesquels il sera possible d'exécuter ses applications.

Remarque :

Le groupe de travail du CIGREF note qu'**il est nécessaire de trouver le bon acteur capable d'accompagner le client**. Et il précise que ce n'est pas facile, car il devra avoir une double casquette : **infrastructure** mais aussi **service** et **usage** pour aider les équipes à gérer et mettre en œuvre sa solution.

Aujourd'hui pour le *IaaS*, on voit se dessiner une offre venant essentiellement des constructeurs, des opérateurs et des hébergeurs.

Cloud & PaaS - Plateform as a Service

Si le *IaaS* concerne essentiellement la production et l'exploitation, le *Cloud* de niveau *PaaS* **concerne les développeurs et les producteurs d'applications**, soit deux niveaux de service : les plateformes de développement, et les applications qui fournissent le service du niveau supérieur (*SaaS*).

Le *PaaS* permet, par exemple, de mettre à disposition des développeurs un ***framework* de développement** adapté à leurs besoins.

Il permet aussi de donner aux applications un **cadre d'exécution** qui produira des services *SaaS* (par exemple Salesforce).

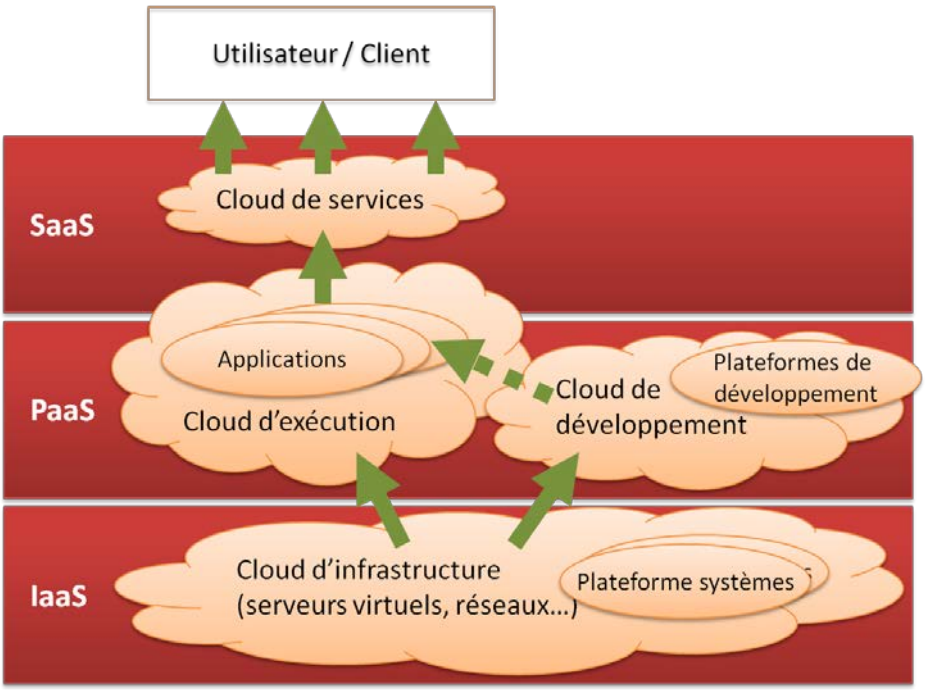
Remarque :

Attention, les ressources requises par une application en mode *PaaS* peuvent dépendre du nombre important de clients qui y accèdent en mode *SaaS* (par exemple pour la consommation de bande passante) et dans ce cas, **le service de fourniture d'une plateforme peut être facturé, par certains opérateurs, comme une plateforme de production classique**, c'est-à-dire au nombre de licences utilisateurs et non pas avec un abonnement global au service.

CLOUD & SAAS - SOFTWARE AS A SERVICE

Le *Cloud* de niveau *SaaS* représente le plus souvent un **catalogue d'applications accessibles en mode service aux utilisateurs ou clients finaux**.

Dans le mode *SaaS*, **l'usage prime sur la solution** : on parle de service de messagerie, de CMS, de service d'achat dans des boutiques en ligne, de service d'accès à des bibliothèques etc. L'application est déjà construite et opérationnelle, il n'y a **pas véritablement de développement mais plutôt du paramétrage** ; d'où le succès de ce modèle de service : il concerne et met à la portée de n'importe qui tout un ensemble de services modelables et personnalisables très simplement.



(Source CIGREF 2013)

Figure 2 : Structuration des différents *Clouds* par rapport au modèle de service

Pour une entreprise, l'utilisation d'un *Cloud* en mode *SaaS* peut être **particulièrement pertinente dans les phases de maquettage ou de prototypage** car cela permet, dans un délai très court et pour un coût réduit, d'évaluer une solution, de pouvoir la tester sans mettre en œuvre des ressources propres, puis de l'internaliser, le cas échéant, si le résultat est concluant.

C'est cette facilité d'usage qui séduit notamment les directions métiers. Elles peuvent, avec ce type de solutions, valider un concept (marketing par exemple), voire en tester plusieurs, faire des choix « métiers » indépendamment du système d'information de l'entreprise ; avec la possibilité d'impliquer immédiatement d'autres acteurs (clients, partenaires) dans la réflexion. Et ceci en s'affranchissant de l'aval de la DSI.

C'est cette facilité d'usage qui inquiète néanmoins la DSI, car elle peut entraîner des choix disjoints de la politique SI de l'entreprise, notamment en termes d'intégration ou de sécurité.

MODÈLE « *AS A SERVICE* » *VS* MODÈLE « *ASP* »

Attention, on peut confondre le « *as a Service* » et ce que l'on appelait auparavant le mode *ASP* (*Application Service Provider*). Si les concepts peuvent paraître proches, il y a des différences notables :

- Les **applications** s'appuyant sur le modèle **« *as a Service* »** ont été nativement conçues pour le web et **utilisent une architecture « *multi-tenant*[13] »**.
    - En mode **« *as a Service* », l'environnement de production est mutualisé et virtualisé** : il n'y a qu'une seule et même instance pour tous les clients. Alors **qu'en mode *ASP*, il y a une instance par client.**
    - En mode ***ASP*, la customisation** est possible mais nécessite **des développements spécifiques** ; **en mode *SaaS*** la **personnalisation** ne peut se faire que **par le paramétrage** car il n'existe qu'un seul et même standard pour tous.
- Les **montées de version en mode *ASP*,** pour les raisons exposées ci-dessus, sont **beaucoup plus complexes**, problématiques (et donc coûteuses) qu'en mode « as *a Service* », *a fortiori* si l'application a fait l'objet de développements spécifiques pour certains clients.
- Pour illustrer la différence entre les deux modes, on peut citer, par exemple, deux solutions leaders sur le marché des applications Achat ayant des modèles complètement différents : Ariba (100% *SaaS*) et Synertrade (100% *ASP*).

LES TYPOLOGIES DU *CLOUD COMPUTING*

Aujourd'hui il n'est pas toujours facile d'avoir une description simple d'un *Cloud* et une explication claire des typologies concernées par les offres des fournisseurs. Il suffit de poser la question « Qu'est-ce qu'un *Cloud* et quelles sont ses typologies ? » lors d'un évènement pour s'en rendre compte. Or la clarté des offres doit contribuer à garantir la qualité des services proposés par la DSI aux directions Métiers clientes.

[13] Une architecture multi-tenant met en œuvre une seule instance d'application, mais utilisable pour tout un ensemble de clients de différentes natures.

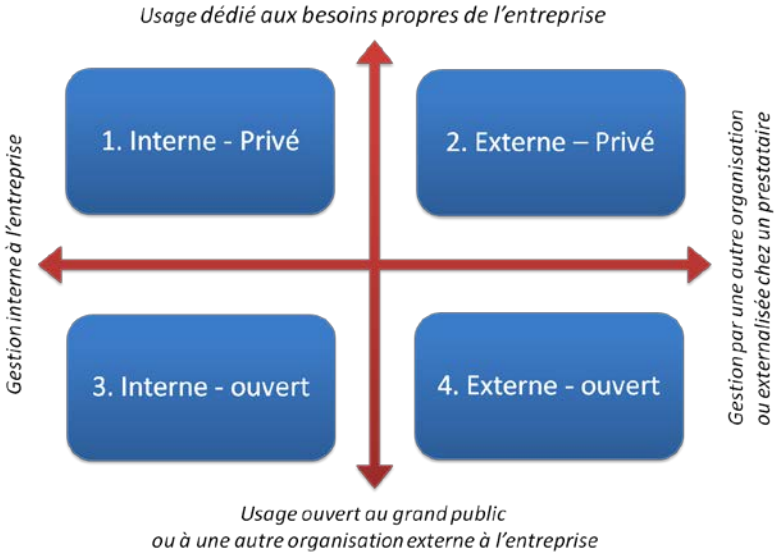
Le groupe de travail du CIGREF s'est donc intéressé aux **différentes typologies de *Cloud Computing*** qui peuvent être mises en œuvre. La réflexion a été organisée autour de deux notions :

1. « **Qui gère le *Cloud* ?** » : l'entreprise elle-même ou un opérateur de *Cloud* ?
   Le groupe a choisi d'utiliser les termes suivants :
   - « *Cloud* **interne** » dans le cas où c'est **l'entreprise qui est maître de la gestion du *Cloud,*** avec ses propres ressources.
   - « *Cloud* **externe** » dans le cas où **la gestion du *Cloud* est maîtrisée par un prestataire opérateur de *Cloud***.

2. « **Qui est le client du service offert par le *Cloud* ?** » : l'entreprise elle-même ou une organisation externe (fournisseur, partenaire, filiale, etc.), voire le grand public (les clients de l'entreprise par exemple) ?
   Le groupe de travail a choisi d'utiliser les termes suivants :
   - « *Cloud* **privé** » s'il est **dédié aux besoins propres de l'entreprise.**
   - « *Cloud* **ouvert** » s'il est **ouvert au grand public** ou à une autre **organisation externe à l'entreprise** (fournisseur, partenaire, filiale etc.)

Au final, **4 typologies ont été identifiées**. Chacune d'elles ne concerne pas toutes les entreprises, mais elles sont représentatives de ce qu'une DSI peut être conduite à envisager.

Les typologies peuvent aussi être mélangées, par exemple un GIE peut gérer un *Cloud* interne, et offrir des services privés pour l'entreprise et publics à d'autres entreprises. De même un *Cloud* interne peut avoir besoin de s'étendre ponctuellement et donc de « déborder » sur un *Cloud* externe : on parlera alors de ***Cloud* hybride**.



(Source CIGREF 2013)

Figure 3 : Les typologies du *Cloud Computing*

1. *Clouds* gérés en interne et à usage privé

Ce sont les **solutions complètement gérées par la DSI**. La DSI peut faire éventuellement appel à un prestataire (type infogérant) mais elle garde la maîtrise complète de la solution.

Les solutions de *Clouds* internes et privés permettent de mettre à disposition un catalogue de services internes et de **se positionner comme une alternative opérationnelle aux services existants sur Internet**.

Elles permettent aussi **une meilleure agilité et une qualité de service accrue**, au détriment peut-être des développements spécifiques qui ne sont plus possibles[14]. Néanmoins comme l'entreprise en a la maîtrise, gérer quelques particularités des clients en personnalisant le paramétrage des instances est toujours possible.

Les retours d'expériences ont aussi montré que la mise en œuvre d'un *Cloud* interne peut permettre **d'optimiser l'utilisation des ressources** d'un *datacenter* et de **pérenniser une infrastructure.**

En termes de sécurité, tous les grands groupes ont défini une politique de sécurité entrant dans le cadre de la gouvernance du SI. Les serveurs supportant un *Cloud* interne sont donc contraints à respecter cette politique de sécurité. Il n'y a donc pas de disposition supplémentaire à prendre.

Voici quelques exemples de *Clouds* internes à usage privé, suivant les couches de service concernées :

- *SaaS* : espaces collaboratifs internes
- *PaaS* : plateformes de serveurs de développement à la demande (développement web : ViFiB)
- *IaaS* : déploiement de serveurs virtuels à la demande (ViFiB, VMware, EMC, IBM, HP, …)

Remarques :

1. **Il y a eu débat au sein du groupe de travail du CIGREF sur l'intérêt de la mise en œuvre d'un *Cloud* Interne à usage privé** pour l'entreprise. Si la plupart des participants au GT conçoivent, dans leur contexte, l'intérêt d'un *Cloud*, d'autres y voient un concept marketing sans réelle valeur ajoutée vis-à-vis des infrastructures traditionnelles. Pour ces derniers, l'intérêt du *Cloud Computing* n'est alors perçu que comme une solution externe à l'entreprise.

[14] Un *Cloud* offre un service générique à l'ensemble de ses clients.

2. Certains membres du groupe de travail pensent aussi qu'il y a **une taille minimum** (pour toutes les couches du modèle de service) **pour qu'un *Cloud* soit utile et efficace** :
   - par exemple un certain nombre de serveurs pour du *IaaS* ;
   - un périmètre applicatif suffisant pour une plateforme *PaaS* ;
   - un catalogue assez étoffé de services pour le *SaaS*.

   Aucun élément quantitatif n'a cependant été donné.

2. *CLOUDS* GÉRÉS EN EXTERNE ET À USAGE PRIVÉ

Ce sont des solutions qui permettent à la DSI de **ne pas investir dans une infrastructure spécifique**, avec les processus accompagnant sa mise en œuvre, et les compétences nécessaires. Cela nécessite néanmoins un minimum d'études et développements indispensables en termes d'intégration avec l'existant[15].

Le **choix d'investissement** dans la mise en œuvre d'un *Cloud* interne *vs* la location de services dans un *Cloud* externe est **lié à la politique à long ou court terme de l'entreprise**, à sa taille, au nombre d'utilisateurs.

Dans cette typologie la relation avec le fournisseur évolue. Des **problématiques nouvelles émergent** en termes de localisation des données, d'interopérabilité des systèmes et de réversibilité des applications. La contractualisation avec le prestataire nécessite alors un point d'attention particulier. **De manière générale, « on n'achète plus une licence, on s'abonne à un service ».**

Dans le cas d'une **location de services**, plusieurs membres du groupe de travail s'accordent à dire qu'elle est **économiquement intéressante sur des durées de quelques semaines ou quelques mois, mais pas sur du long terme**. Quand le modèle de licence est possible, le ROI[16] semble plus intéressant sur du long terme, mais avec l'évolution des technologies, des usages, et surtout des politiques d'entreprises, **il n'est pas possible de se projeter au-delà de 3/4 ans.** L'abonnement prévaut donc avec succès.

En termes de sécurité, la problématique du *Cloud* externe est différente de celle du *Cloud* interne : la politique de sécurité du fournisseur n'est pas maitrisée par le client. Or dans ce cas précis, **le fournisseur doit pouvoir garantir la sécurité des données du client**. Il doit avoir une gouvernance adaptée au client, sinon il y a risque d'allégeance à la politique du fournisseur. La question est donc de savoir **comment influencer un fournisseur de *Cloud***

[15] Le *legacy*

[16] ROI : *Return Of Investment* (retour sur investissement)

pour que le contrat ne soit pas complètement générique, notamment sur les questions de sécurité des données[17].

L'usage d'un *Cloud* externe et privé implique aussi de bien **définir le périmètre des services attendus**. Ce périmètre doit aller **au-delà des services logiciels et techniques**, il doit pouvoir englober des expertises métier pour être performant et pertinent dans les phases de paramétrage, formation et conduite du changement. Si ces prestations métier peuvent faire l'objet d'un contrat de prestations avec une société de conseil, il semble préférable de **responsabiliser le fournisseur de la solution** en lui confiant une responsabilité de maître d'œuvre avec une obligation de bonne fin.

Enfin, une zone d'ombre persiste, liée au modèle en couches : **le prestataire s'engage sur la couche de service concernée par le contrat, mais qu'en est-il des couches inférieures[18] ?** Aucune réponse n'a pour le moment été trouvée dans les différentes offres.

Voici quelques exemples de *Clouds* externes à usage privé suivant les couches de service concernées :

- *SaaS* : Suites bureautiques en ligne (Google Apps, Office 365), CRM (Salesforce), services de vente en ligne (Amazon)
- *PaaS* : Environnements de développement (Oracle PaaS, Salesforce, ViFiB, …)
- *IaaS* : Location d'infrastructures virtuelles (OVH, Amazon, Numergy, CloudWatt, Cheops Technology, Intrinsec, …)

3. *Clouds* gérés en interne et à usage ouvert

Cette typologie concerne le plus souvent les organisations (comme les GIE[19]) qui offrent des services en interne à l'entreprise et en externe à des clients. **L'entreprise est alors elle-même « Opérateur de *Cloud* ».**

Dans ce cas de figure, les contraintes et remarques identifiées précédemment pour un Cloud externe à usage privé, s'appliquent mais de manière inversée :

- Savoir répondre aux problématiques de localisation des données, d'interopérabilité des systèmes et de réversibilité des applications.
- Bien choisir le modèle économique : licence ou abonnement.

[17] A ce sujet, de plus amples informations se trouvent dans le rapport (à paraitre) CIGREF/AFAI/IFACI « *Cloud Computing* et protection des données. Guide pratique à l'attention des directions générales et opérationnelles »

[18] Hormis le *IaaS* qui est la couche la plus basse.

[19] GIE : Groupement d'Intérêt Économique

- S'appuyer et communiquer sur sa propre gouvernance de la sécurité pour garantir la sécurité des données de son client.
- Déterminer le périmètre des services offerts.
- Apporter une réponse sur l'engagement sur les couches de services inférieures à celle du service proposé.

Voici quelques exemples de *Clouds* internes à usage ouvert suivant les couches de service concernées :

- *SaaS* : site web clé en main de type CMS pour une entreprise franchisée
- *PaaS* : offre de plateforme de développement à la demande (Free Cloud Alliance, …), paramétrage de configuration virtuelle (VMWare, …)
- *IaaS* : offre de serveurs virtualisés (VMWare, IBM, HP, Free Cloud Alliance, …)

4. *CLOUDS* GÉRÉS EN EXTERNE ET À USAGE OUVERT

Cette typologie correspond, par exemple, aux cas des directions Métiers qui s'adressent directement aux opérateurs de service, pour mettre en place un *Cloud* de service à destination de populations externes à l'entreprise comme les clients ou les partenaires.

Cette situation, reconnue par de nombreuses entreprises membres, est donc **singulière** car elle permet aux directions métiers de « s'affranchir », *a priori*, de la DSI. Cette typologie permet aussi souvent aux directions Métiers de **challenger la DSI dans sa capacité à offrir un service équivalent** en termes d'usage, de coût, de délai et de performances.

Au-delà de la communication nécessaire entre la DSI et les directions métiers, le rôle de la DSI est donc dans ce cas, de conseiller le client dans le choix du *Cloud* approprié à son besoin, d'éviter les redondances avec le système d'information existant, ou les trous de sécurité inopinés créés par des raccords « sauvages » sur le SI de l'entreprise.

Voici quelques exemples de *Clouds* externes à usage ouvert suivant les couches de service concernées :

- *SaaS* : réseaux sociaux publics ou professionnels (Facebook, Google+, LinkedIn), publication ou mise en ligne de produits dans des magasins numériques (AppleStore, Amazon)
- *PaaS* : plateformes de développement d'applications mobiles (Kawet), paramétrage de configuration virtuelles (VMware), ou d'hébergement d'applications (Windows Azure), développement web (ViFiB)
- *IaaS* : espaces de stockage de données (iCloud, SkyDrive, Google Drive, DropBox, CloudWatt, Numergy, opérateurs télécoms : Orange, SFR, Bouygues Telecoms…)

CONSEILS ET BONNES PRATIQUES

Les tableaux qui suivent contiennent un ensemble de conseils et de bonnes pratiques concernant les 4 typologies de *Cloud*. Cette liste n'est pas exhaustive, elle est issue des multiples échanges et retours d'expérience effectués lors des réunions du groupe de travail.

Ces conseils et bonnes pratiques ont été regroupées en 5 catégories :

A. Juridique
B. Sécurité et risques
C. RH et compétences
D. Données et audit
E. Infrastructures

1. *Cloud* Interne – Privé *L'entreprise gère un Cloud pour son usage interne*	2. *Cloud* Externe – Privé *L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne*
A. JURIDIQUE	
CONTRAT	
• Veiller aux contrats avec les éditeurs et constructeurs (notamment la structure tarifaire des licences et la dépendance avec l'infrastructure) pour les logiciels déployés sur le *Cloud* Interne. • Etablir une « offre de service » interne pour cadrer les prestations et engagements vis-à-vis des usagers internes.	• Veiller aux contrats avec les opérateurs de *Cloud*, et notamment que l'opérateur fournit des niveaux de service différenciés (SLA). • Contractualiser un engagement d'assistance du fournisseur pour une récupération des données (en cas de faillite, fin de contrat…). • Veiller aux contrats de licence pour les logiciels déployés sur le *Cloud*. Attention, un contrat « *SaaS* » ou « *ASP* » est assez complexe à construire car il doit reposer sur des obligations relevant de différents types de contrats (contrat de licence, TMA, infogérance, hébergement, assistance technique…). • Si le fournisseur d'une solution *SaaS* utilise des modules applicatifs qui ne lui appartiennent pas, il faut bien s'assurer que le ou les fournisseurs de ces modules sont engagés contractuellement sur toute la durée de votre propre contrat.

1. *Cloud* Interne – Privé ***L'entreprise gère un Cloud pour son usage interne***	2. *Cloud* Externe – Privé ***L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne***
RESPONSABILITÉ	
• Couvrir les risques d'un usage détourné de la donnée (ex : charte IT interne à l'entreprise, annexe spécifique dans les conditions contractuelles d'achat de prestation). • Définir les moyens permettant d'identifier les responsabilités en cas de perte ou d'altération de la donnée (traçabilité, contrôle, audit…).	• Obtenir de l'opérateur des garanties ou *a minima* les modalités mises en œuvre pour couvrir les risques d'un usage détourné de la donnée. • Exiger que les responsabilités puissent être déterminées en cas de perte ou d'altération de la donnée.
PRIX	
• S'assurer que les prix/conditions sont garantis dans le temps (notamment dans le cas du rachat du fournisseur par un autre...) • S'assurer que les prix sont bien assujettis sur un usage « *on demand* » c'est-à-dire que l'on peut réduire le nombre d'utilisateurs et donc les frais (mensuels, annuels) si l'activité le justifie.	
RÉVERSIBILITÉ	
	• Formaliser les conditions de réversibilité.
PROPRIÉTÉ	
	• S'assurer de la propriété intellectuelle sur les processus métier et les données de l'entreprise qui sont sur le *Cloud*. • Avoir des garanties quant à la propriété et la localisation des données (en termes de pays pour les aspects de réglementation). • Évaluer l'impact du *Patriot Act* dans le cas d'un prestataire américain.

1. *Cloud* Interne – Privé *L'entreprise gère un Cloud pour son usage interne*	2. *Cloud* Externe – Privé *L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne*
B. SÉCURITÉ & RISQUES	
PRA/PCA	
• Repenser et adapter les procédures de PRA/PCA Métier internes à l'entreprise.	• Prévoir les tests de PRA. • Repenser et adapter les procédures d'ouverture et de synchronisation des flux ainsi que les procédures de PCA Métier internes à l'entreprise. • *Remarque : Vérifier l'applicabilité d'un PRA/PCA implique de s'assurer au préalable que c'est possible avec la solution externe proposée.*
GARANTIES	
	• Obtenir des garanties sur les délais de reconstruction à flux fermés des applications externalisées. • Réexaminer les contraintes et recommandations de la CNIL au regard de l'environnement externalisé.
CONTRAINTES PRESTATAIRE	
	• Exiger du prestataire qu'il soit certifié ISO 27001 ou label SAS 70 type II afin de garantir aux utilisateurs que toutes les obligations de sécurité sont bien respectées. • Exiger du prestataire la liste de tous les lieux de stockage des données, y compris les sites de secours.

1. *Cloud* Interne – Privé ***L'entreprise gère un Cloud pour son usage interne***	2. *Cloud* Externe – Privé ***L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne***
C. RESSOURCES HUMAINES	
COMPÉTENCES	
• Besoin de compétences plutôt techniques, support et virtualisation. Certaines compétences peuvent évoluer d'un profil d'opérateur technique vers un profil d'analyste ou de développeur d'automatismes. • Disposer de compétences métiers permettant de comprendre et d'anticiper les besoins et les usages que les métiers peuvent faire d'un *Cloud*, pour éviter par exemple qu'ils fassent appel à un *Cloud* externe.	• Même si on a moins besoin de compétences techniques et de support aux opérations il faut conserver un noyau d'expertise technique, notamment dans le cadre des réversibilités ou du déclenchement de PRA/PCA. • Renforcer les compétences en matière de contrat, d'achat et de juridique. • Se recentrer sur le métier tout en conservant le volume de compétences techniques clés en interne, pour la gestion des infrastructures internes restantes, pour garantir l'interopérabilité entre l'interne et l'externe. • L'implication et, surtout, la disponibilité des utilisateurs sont essentielles pendant les phases de paramétrage, recette et migration. Le déploiement d'un projet *SaaS* sans la mobilisation des clients utilisateurs de l'outil est voué à l'échec. • Le succès du déploiement d'une solution *SaaS* est notamment proportionnel à l'investissement réalisé dans la conduite du changement (information, formation, communication, coaching …). • Un fournisseur d'une solution *SaaS* doit avoir des compétences métier en rapport avec l'application qu'il fournit, c'est là sa vraie valeur ajoutée. Le fournisseur ne doit pas seulement se contenter de mettre à disposition du client un outil, il doit aussi apporter de la valeur « *business* » permettant au client d'automatiser et d'optimiser ses processus. Dans certains cas, la

1. *Cloud* Interne – Privé *L'entreprise gère un Cloud pour son usage interne*	2. *Cloud* Externe – Privé *L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne*
	solution *SaaS* à valeur ajoutée (accompagnée de services métier) peut même répondre à des besoins de *Business Process Outsourcing* (BPO) pour les entreprises qui souhaitent externaliser tout ou partie de leurs fonctions métiers (Finance, RH, Achat …). • Les compétences métier du prestataire sont très importantes pendant la phase de paramétrage de l'outil. Cette phase ne doit pas être négligée car elle correspond à la phase de « conception » de l'outil. Et au cours de cette phase, il peut être très utile de travailler sur la rationalisation, la standardisation, voire l'optimisation des processus métier existants, avant de se lancer tête baissée dans le paramétrage.
ORGANISATION	
• Attention, certaines solutions *Cloud* concentrent les responsabilités techniques et financières : une modification dans le *Cloud peut* alors déclencher immédiatement un engagement financier. • La mobilité des utilisateurs est offerte par les services d'un *Cloud*, cela peut avoir des impacts sur les contrats de travail.	

1. *Cloud* Interne – Privé *L'entreprise gère un Cloud pour son usage interne*	2. *Cloud* Externe – Privé *L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne*
D. DONNÉES & AUDIT	
AUDIT	
• Pas de modification particulière par rapport à une exploitation interne traditionnelle.	• Prévoir les conditions d'audit de la sécurité et du service. • Prévoir dans le contrat une clause d'audit technique et d'accès aux locaux du prestataire.
LOCALISATION	
	• L'opérateur du *Cloud* doit pouvoir fournir des informations sur la localisation des données dans ses *datacenters.* • L'opérateur doit pouvoir garantir les risques d'un usage détourné de la donnée.
RESPONSABILITÉ	
	• L'opérateur doit être en mesure de déterminer les responsabilités en cas de perte ou d'altération de la donnée.
DONNÉES	
	• S'assurer que l'opérateur puisse garantir à l'entreprise cliente la conservation de la propriété intellectuelle sur les processus métier et les données du client. • Si des données à caractère personnel sont gérées sur les serveurs du

1. *Cloud* Interne – Privé *L'entreprise gère un Cloud pour son usage interne*	2. *Cloud* Externe – Privé *L'entreprise utilise un Cloud géré par un opérateur externe pour son usage interne*
	fournisseur, le client doit procéder à l'ensemble des obligations qui lui incombent dans le cadre de la loi de janvier 1978 « Informatique & Liberté ». Des autorisations CNIL sont donc nécessaires (même dans le cas d'un *Cloud* externe privé). • Dans le cas où les données sont stockées sur des serveurs localisés dans des pays en dehors de l'Union Européenne, une autorisation spéciale de transfert des données doit être demandée à la CNIL. • Migration des données : préparer les données à migrer, mais laisser au prestataire la responsabilité de la migration. « Le diable est dans le détail » et en matière de migration, il n'y a que des détails à gérer.
E. INFRASTRUCTURES	
• La solution s'appuie sur le réseau de l'entreprise. • L'entreprise doit garder la maîtrise de l'intégration de la solution *Cloud* dans l'infrastructure existante. • L'entreprise doit garder la maitrise de la structure tarifaire des licences des outils constituant le *Cloud*.	• Etre vigilant sur le réseau informatique qui donne accès au fournisseur de *Cloud* : qualité de service, disponibilité, mesures… • Savoir faire face aux mises à niveau de l'infrastructure restée internalisée, induites par les évolutions techniques du *Cloud* externe (en particulier sur les postes de travail). • Vérifier qui gère les infrastructures du *Cloud* : l'opérateur lui-même ou l'un de ses sous-traitants. Dans ce dernier cas, demander à avoir des informations sur le contrat qui les lie.

3. *Cloud* Interne – Ouvert ***L'entreprise gère un Cloud ouvert vers des organisations externes ou le grand public***	4. *Cloud* Externe – Ouvert ***L'entreprise utilise un Cloud géré par un opérateur externe pour un usage tourné vers des organisations externes ou le grand public***
A. JURIDIQUE	
CONTRAT	
• L'entreprise offrant un service de *Cloud*, elle doit s'interroger sur les modalités du service qu'elle offre. Font-elles partie d'une offre globale ou peuvent-elles être négociables ?	• Les modalités du contrat dépendent de l'offre fournisseur, elles peuvent être difficilement négociables. • L'offre *multi-device* (notamment sur les outils mobiles) est souvent présente pour répondre au marché mais il n'est pas garanti qu'elle fasse réellement partie du contrat.
RESPONSABILITÉ	
• Préciser les engagements de l'entreprise en termes de PRA. • Bien déterminer le périmètre de responsabilité du client du *Cloud* en cas de PRA/PCA. • Dans la négociation d'un SLA avec le client, définir le périmètre de l'administration fonctionnelle le cas échéant. • Définir les modalités de publication de la *roadmap* technique de l'entreprise afin de permettre aux clients de préparer et mettre en œuvre les adaptations le cas échéant.	• Fournir un PRA/PCA implique de s'assurer au préalable que c'est possible avec la solution externe proposée. • L'entreprise ne maîtrise pas l'évolution de la plateforme, elle doit donc se tenir informée de la *roadmap* de la solution administrée pour en informer ses clients.

3. *Cloud* Interne – Ouvert ***L'entreprise gère un Cloud ouvert vers des organisations externes ou le grand public***	4. *Cloud* Externe – Ouvert ***L'entreprise utilise un Cloud géré par un opérateur externe pour un usage tourné vers des organisations externes ou le grand public***
RÉVERSIBILITÉ	
• Définir les formats supportés pour la restitution de données.	• Définir les formats supportés pour la restitution de données. • Garantir au client une réversibilité des données implique de s'assurer au préalable que c'est possible avec la solution externe proposée.
INTEROPÉRABILITÉ	
• L'interopérabilité de la plateforme dépend des choix d'architecture interne à l'entreprise et doit s'adapter aux besoins des clients. • La mise en œuvre de solution *Open source* dans un *Cloud* interne nécessite de définir un processus d'information, vers les clients, sur les licences.	• L'interopérabilité de la plateforme dépend de la solution choisie. • Pour un *Cloud* externe, il est difficile de savoir si des modules *Open source* sont mis en œuvre, lesquels et leurs modes de licence ; et donc de prévoir les incidences sur les clients.
PRIX	
• L'entreprise peut définir son *pricing* en fonction de critères maîtrisés (investissement, usage, volumétrie, niveau de service, besoins des clients etc.), mais attention à la dépendance tarifaire avec certains fournisseurs, notamment les éditeurs des logiciels constituant le *Cloud*.	• L'entreprise qui utilise un *Cloud* externe ouvert est dépendante des prix pratiqués par son opérateur de *Cloud*. Dans le cas où elle offre un service externe à l'entreprise, elle peut être amenée à le faire payer. Sa tarification devra suivre celle de son opérateur.

3. *Cloud* Interne – Ouvert *L'entreprise gère un Cloud ouvert vers des organisations externes ou le grand public*	4. *Cloud* Externe – Ouvert *L'entreprise utilise un Cloud géré par un opérateur externe pour un usage tourné vers des organisations externes ou le grand public*
B. SÉCURITÉ & RISQUES	
AUDIT	
• Une solution interne doit être auditable et soumise à des tests d'intrusion.	
DONNÉES	
• La loi française impose à une entreprise offrant un espace de stockage de données, la connaissance de la localisation des données. • S'interroger sur la possibilité d'assurer le client que ses données ne sont reconstituables que par lui (pour éviter l'accès d'un tiers). • La traçabilité, l'archivage et la réversibilité doivent être garantis en termes de sécurité. • S'assurer du respect de la réglementation auprès de la CNIL. • Les garanties à offrir à un client sont celles que l'entreprise exigerait si elle s'appuyait sur un opérateur de *Cloud* externe.	• La loi française impose à une entreprise offrant un espace de stockage de données, la connaissance de la localisation des données. Mais si la solution n'est pas fournie par un opérateur français, la localisation des données n'est pas garantie. • La solution externe choisie doit répondre aux contraintes de la CNIL. • La garantie de l'accès par l'entreprise à la reconstitution de ses données (pour éviter l'accès d'un tiers) dépend de la solution choisie. • La traçabilité, l'archivage et la réversibilité dépendent de la solution choisie. Il est difficile pour l'entreprise offrant le service de les garantir. • Une solution externe peut être soumise à des tests d'intrusion mais est difficilement auditable car la localisation des données est difficilement possible.

3. *Cloud* Interne – Ouvert ***L'entreprise gère un Cloud ouvert vers des organisations externes ou le grand public***	4. *Cloud* Externe – Ouvert ***L'entreprise utilise un Cloud géré par un opérateur externe pour un usage tourné vers des organisations externes ou le grand public***
C. RESSOURCES HUMAINES	
COMPÉTENCES	
• Pour un *Cloud* interne, les compétences sont plutôt techniques, support et virtualisation. • Certaines compétences peuvent évoluer d'un profil d'opérateur technique vers un profil d'analyste ou de développeur d'automatismes. • La mobilité des utilisateurs est offerte par les services d'un *Cloud*, cela peut avoir des impacts sur les contrats de travail.	• Pour un *Cloud* externe, les compétences couvrent les aspects techniques et support, mais aussi achat et juridique.
D. AUDIT & DONNÉES	
DONNÉES	
• L'entreprise doit pouvoir fournir des informations sur la localisation (géographique) des données dans ses propres *datacenters.* • Couvrir les risques d'un usage détourné de la donnée.	• Obtenir les informations sur la localisation (géographique) des données. • L'entreprise doit s'informer sur ses moyens d'action sur la solution en cas d'un usage détourné de la donnée.

3. *Cloud* Interne – Ouvert ***L'entreprise gère un Cloud ouvert vers des organisations externes ou le grand public***	4. *Cloud* Externe – Ouvert ***L'entreprise utilise un Cloud géré par un opérateur externe pour un usage tourné vers des organisations externes ou le grand public***
RESPONSABILITÉ	
• L'entreprise est responsable en cas de perte ou d'altération de la donnée. • Garantir la conservation de la propriété intellectuelle sur les processus métier et les données du client.	• S'informer sur la responsabilité de l'entreprise en cas de perte ou d'altération des données. • Étudier l'impact du *Patriot Act* dans le cas d'un prestataire américain. • S'assurer de la conservation de la propriété intellectuelle sur les processus métier et les données du client.
E. INFRASTRUCTURES	
• L'interopérabilité de la plateforme dépend des choix d'architecture interne à l'entreprise et peut s'adapter aux besoins des clients. Il faut toutefois veiller à respecter les standards simples du marché en termes d'accès ou d'échange. • L'offre *multi-device* (notamment sur les outils mobiles) n'est pas simple à mettre en œuvre car il faut la développer (il y a de nombreux *devices* différents et il en apparaît régulièrement) et la maintenir dans le temps (les *devices* évoluent très rapidement).	

CONCLUSION

Le *Cloud Computing* est aujourd'hui un élément clé de la transformation numérique des entreprises. Il permet à ces dernières de se dégager de la contrainte technique au profit de l'agilité et de l'adaptation du service aux besoins des Métiers. Il permet aussi de répondre efficacement à la problématique de la mobilité en donnant accès aux informations et services en tous lieux.

Au-delà des différentes définitions identifiées par le groupe de travail, qui sont nécessaires pour échanger et faciliter la compréhension entre les différentes parties prenantes, le défi de la DSI est de savoir marier les 4 typologies du *Cloud Computing* décrites dans ce rapport. De fait, les entreprises devront, si ce n'est déjà fait, faire cohabiter des solutions externes et internes, ouvertes et privées.

Dans ce patchwork de solutions qui s'installent dans le SI de l'entreprise, la valeur ajoutée de la DSI est d'y mettre de la cohérence, d'architecturer les services et de garantir une qualité de service constante et équivalente en externe comme en interne. C'est aussi de pérenniser l'infrastructure et l'architecture du SI en les transformant pour faire face à l'évolution de la stratégie de l'entreprise mais aussi de l'environnement dans lequel elle évolue.

Dans ce cadre, le rôle de la DSI pourrait évoluer vers un rôle de « courtier » qui propose ses propres services internes mais aussi encapsule des services externes pour les intégrer et les proposer en interne. Le challenge est, en s'appuyant sur une relation avec des métiers de plus en plus mature, d'être suffisamment en amont des besoins (une veille auprès des directions Métiers est indispensable) pour fournir et intégrer, s'ils sont pertinents, les services, tout en maitrisant la sécurité, l'interopérabilité, etc.

Ce challenge comprend aussi l'établissement d'un contrat qui, tout en protégeant le SI et l'entreprise vis-à-vis de ses fournisseurs, garantit la préservation du service sur l'accès, la qualité et les données, ainsi que la réversibilité, et ceci au-delà de la période contractuelle (dans le cas d'un changement de contrat, les données doivent toujours être accessibles tant que la migration n'a pas eu complètement lieu).

> *« … L'émergence du cloud computing et des services associés constitue une mutation qui se traduit par des modèles économiques différents et des offres nouvelles ayant un impact important sur l'écosystème des services d'information des entreprises… Le cloud computing est une solution à combiner aux solutions SI existantes. La fonction SI a un rôle d'intégrateur ultime avec les processus métiers et les autres solutions constituant le patrimoine applicatif de l'entreprise étendue. Les offres de cloud computing doivent donc être interopérables, réversibles et reposer sur des standards ouverts. L'offre de cloud computing doit être source d'innovation pour les entreprises, en termes de financement, de sourcing, d'architecture et surtout de services différenciés…* »
>
> L'Entreprise numérique – *Quelles stratégies ? (décembre 2010)*

CIGREF

21 avenue de Messine

75008 PARIS

Tel. : +33 1 56 59 70 00

Fax : +33 1 56 59 70 01

cigref@cigref.fr

www.cigref.fr