cigref Réseau de Grandes Entreprises

ifaci institut français de l'audit et du contrôle internes

AFAI® Pour des systèmes d'information de confiance et créateurs de valeur

GUIDE PRATIQUE

Cloud computing et protection des données

Guide pratique
à l'attention des directions générales et opérationnelles

Sommaire

Avant-Propos

Le présent document « *Cloud Computing* et protection des données » est le fruit d'un travail collectif qui a mobilisé trois associations : le CIGREF, l'IFACI et l'AFAI, pendant six mois, avec les contributions des personnes suivantes :

- ANTONINI Pascal Ernst & Young - Président de l'AFAI
- BOUTEILLER Sophie CIGREF
- BOUTIN Matthieu CIGREF
- DELAYAT Régis SCOR – Administrateur du CIGREF et de l'AFAI
- GARCIA Christine Renault
- GUIHEUX Henri SCOR
- HERVIAS Philippe Sanofi
- KI-ZERBO Béatrice Béatrice
- LE ROUX Yves CA
- MALAGOLI Frédéric Ernst & Young
- MENCEL Marc Nexter Group
- NICOLAS Guy Nexans
- SZNIKIES Olivier Lafarge

Parallèlement aux travaux menés sur la protection des données en *Cloud Computing* (objet du présent document), le CIGREF a conduit des travaux plus techniques sur le *Cloud Computing*. Les quatre typologies de *Cloud Computing* reprises dans les pages suivantes sont issues des réflexions de ce second groupe de travail CIGREF.

L'expression française...

- Pour *Cloud Computing* : « Informatique en nuage »
- Pour SaaS : *Software as a Service* : « logiciel à la demande »

Synthèse

Avec la révolution numérique, l'information est devenue l'une des principales richesses de l'entreprise, à condition toutefois qu'elle soit maîtrisée, c'est-à-dire collectée, validée, stockée, sécurisée, aisément accessible aux seules personnes intéressées, traitée et agrégée pour des prises de décision avisées. La protection de cette information est au cœur des préoccupations des entreprises. C'est une problématique en soi, tous les jours un peu plus prégnante, du fait du développement pléthorique des données, structurées et non structurées, et du renforcement des contraintes réglementaires. Le contexte spécifique du *Cloud*, où les données sont hébergées à l'extérieur de l'entreprise, exacerbe cette préoccupation.

Le mouvement vers le *Cloud* semble inéluctable, il ne s'agit pas ici de s'y opposer, mais d'alerter et d'inciter les entreprises qui font ce choix, de le faire avec la certitude que leurs données seront correctement protégées. Le CIGREF, l'IFACI et l'AFAI se sont conjointement mobilisés pour concevoir ce guide, dont l'objectif est de sensibiliser tous les acteurs de l'entreprise, et en particulier les dirigeants, directeurs Métiers, auditeurs, à la problématique de la protection des données, personnelles et sensibles, dans les projets *Cloud*. Le groupe de travail a réuni des représentants des trois associations, issus de DSI, de directions de l'audit interne, et de cabinets d'audit et de conseil.

L'approche commune s'articule autour de quatre messages clés :

- Le *Cloud* présente de nombreux avantages d'agilité, de souplesse et de réduction des coûts, mais l'offre actuelle de *Cloud* est susceptible d'exposer les entreprises à des risques sur leurs données
- Il est important de s'engager dans le *Cloud* avec ses différentes parties prenantes : les Métiers, la DSI, les Achats, l'Audit interne, le Juridique, le *Risk Management*, le Contrôle Interne…
- Il est important de se poser les bonnes questions pour faire les bons choix : quel *Cloud* pour quel usage ?
- Il faut mettre en place un environnement de contrôle adapté pour assurer la protection des données dans le respect du cadre contractuel défini avec le fournisseur.

Ce document vise à apporter un service concret aux entreprises prêtes à s'engager dans le *Cloud*, avec des exemples pratiques (questions à se poser avant de prendre la décision, clauses contractuelles, objectifs de contrôle opérationnel…). Il s'adresse certes aux acteurs de l'entreprise (Directions Générales, Directions Métiers) mais aussi aux fournisseurs de solutions *Cloud*, qui doivent mieux prendre en compte cette problématique de protection des données et renforcer leurs garanties en la matière.

Préambule

Pour aborder la notion de protection des données dans le *Cloud*, il est important de la relier d'abord aux enjeux des Métiers. Cette réflexion sur l'analyse du risque encouru peut ainsi se structurer à partir de la question « quel *Cloud* pour quel usage ? ». Il s'agit donc de déterminer le niveau de protection nécessaire aux données hébergées, quelle que soit leur localisation, et de choisir l'offre la plus adaptée à l'usage souhaité.

Par ailleurs, force est de constater que cette nouvelle offre de *Cloud,* pour s'imposer sur un marché de masse, a centré sa communication sur la mise en valeur d'avantages incontestables en matière d'agilité, de capacité de réponse rapide à un besoin opérationnel, de réduction importante des coûts de déploiement et d'usage, et d'élasticité de l'offre, c'est-à-dire la capacité de s'ajuster au plus près de la croissance ou décroissance du besoin. Ainsi, l'aspect de la protection des données est, dans les faits, passé au second plan chez les fournisseurs de *Cloud*.

Par ailleurs, le retour d'expérience des entreprises montre que les offres actuelles de *Cloud* n'apportent pas un niveau de garantie satisfaisant en matière de protection des données confidentielles ou à caractère personnel.

Enfin, l'offre *Cloud* pour le grand public et les avantages énoncés plus haut, sont une incitation permanente des directions Métiers à s'affranchir des contraintes liées au recours aux Directions Systèmes d'Information internes des entreprises, sans qu'elles mesurent l'impact potentiel de telles initiatives sur les Métiers ou sur l'efficacité et la performance du système d'information.

C'est pourquoi la sélection de l'offre *Cloud* la plus adaptée au besoin relève d'abord des opérationnels, et doit être effectuée en lien avec les informaticiens. Ce guide pratique facilitera leur dialogue en clarifiant ce que sont les offres *Cloud* disponibles, ce qu'est la réalité de ces offres, et leurs limites en matière de protection des données. Il permettra également d'accompagner les entreprises, en listant les questions à se poser avant leur prise de décision, et les précautions contractuelles et opérationnelles à prendre.

Termes clés

Vous trouverez ci-après une brève description des différents modèles de services d'une part, et des différents types de *Cloud* d'autre part.

Modèles de services

IaaS (Infrastructure as a Service)

L'Infrastructure en tant que Service est un modèle de *Cloud computing* où l'entreprise dispose d'une infrastructure informatique hébergée chez le fournisseur. Ainsi :

- L'entreprise maintient ses applications, et la plateforme d'exécution de ces applications (bases de données, logiciel serveur) ;
- Le fournisseur de *Cloud* maintient l'infrastructure (virtualisation, matériel serveur, stockage et réseaux).

PaaS (Platform as a Service)

La Plateforme en tant que Service est un modèle de *Cloud computing* où l'entreprise dispose d'un environnement dans lequel la plateforme d'exécution de ses applications (bases de données, logiciel serveur) est totalement externalisée. C'est une « boîte noire ». Dans ce cas :

- L'entreprise maintient uniquement ses applications ;
- Le fournisseur de *Cloud* maintient la plateforme d'exécution de ces applications et l'infrastructure.

SaaS (Software as a Service)

Le Logiciel en tant que Service est un modèle de *Cloud computing* où l'entreprise est utilisatrice d'une ressource informatique (infrastructure, plateforme et applications) totalement externalisée :

- L'entreprise s'abonne à une application en ligne, comme par exemple la messagerie électronique (gmail, yahoo mail…), plutôt que d'acheter une licence ;
- Le fournisseur de *Cloud* maintient les applications qu'il propose, la plateforme d'exécution de ces applications ainsi que les infrastructures sous-jacentes.

Les offres de type IaaS ou PaaS s'adressent davantage aux Directions Systèmes d'Information, qu'aux Directions Métiers.

Ce guide pratique met l'accent sur la protection des données pour les offres de *Cloud*s de type SaaS, offres qui s'adressent directement aux directions opérationnelles et générales des entreprises.

Face à des offres commerciales très dynamiques et mouvantes, nous proposons comme grille de lecture et d'aide à la décision, quatre catégories principales d'offres de *Cloud*, prises du point de vue de l'entreprise utilisatrice.

Les principaux types de *Cloud* proposés

Le *Cloud* se définit de la manière suivante (source CIGREF) :

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.

Quatre typologies de *Cloud Computing* peuvent alors être décrites.

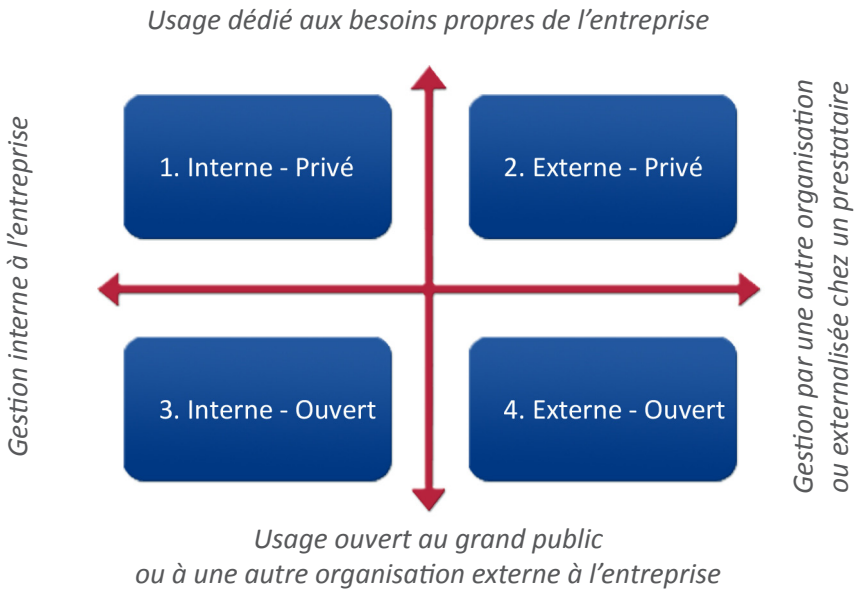

Figure 1 - Typologie des clouds (source CIGREF 2013)

Cloud géré en interne et à usage privé (Type 1)

Il s'agit ici de la fourniture de services informatiques basés sur les technologies de virtualisation au sein d'une entreprise.

Pour les organisations dont la taille est suffisante pour en justifier l'investissement, la mise en place d'un *Cloud* interne privé représente une opportunité d'économie et de mutualisation des infrastructures SI au service de l'agilité et de la souplesse de mise en place des applications métiers de l'entreprise.

Dans ce cas, le dispositif de protection des données est comparable à celui rencontré par toute organisation opérant son système d'information selon des modalités classiques en interne à l'entreprise.

Cloud géré en externe et à usage privé, souvent qualifié de « cloud privé » par les fournisseurs (Type 2)

Certains fournisseurs de solutions métiers proposent des offres clés en main qui reposent, de plus en plus souvent et de façon plus ou moins explicite, sur une infrastructure de type *Cloud*.

A la différence des *Cloud*s publics, ces solutions intégrées sont hébergées sur l'infrastructure privée du fournisseur de service, mais l'usage de ces infrastructures reste partagé entre plusieurs entreprises clientes, dans un nombre limité.

Dans cette catégorie, on distingue le cas particulier du *Cloud* communautaire qui réunit des organisations ayant des besoins communs auxquels le *Cloud* apporte une réponse mutualisée. On peut citer par exemple Amadeus pour le traitement des réservations de voyage.

Cloud géré en interne et à usage ouvert (Type 3)

Cette typologie concerne le plus souvent les GIE qui offrent des services en interne à l'entreprise (mère) 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 (type 2) s'appliquent, mais de manière inversée (l'entreprise ou le GIE informatique devient fournisseur de *Cloud*).

Cloud géré en externe et à usage ouvert (Type 4)

Il s'agit de services gratuits ou payants de stockage et d'applications Web destinés le plus souvent au grand public. Ces services sont accessibles via le réseau internet, en libre-service ou payants.

L'application la plus répandue est la messagerie électronique - Yahoo, Gmail - mais des suites bureautiques sont également disponibles, par exemple l'offre Google Apps ou Microsoft 365.

Ce modèle de solution souvent nommé *Cloud* public repose sur la disponibilité en ligne des applications et des données de l'utilisateur final. Les données sont gérées par le fournisseur de *Cloud*, sans visibilité pour le client sur les modalités de conservation de celles-ci : elles peuvent être stockées aussi bien sur les infrastructures informatiques mutualisées du fournisseur lui-même, que chez l'un de ses sous-traitants. Ces infrastructures sont par ailleurs bien souvent réparties dans des *datacenters* implantés dans différents pays, rendant peu prédictible la localisation des données de l'utilisateur, ce qui peut être rédhibitoire pour la gestion de données dont la géolocalisation est primordiale (par exemple les données à caractère personnel d'une entreprise).

Les données stockées sur ces solutions *Cloud* peuvent, dans la plupart des cas, bénéficier d'un statut « privé », mais la robustesse de la protection reste limitée le plus souvent à celle d'un mot de passe. Le fournisseur s'engage sur la disponibilité de l'accès aux données et moins sur la protection de cet accès.

Le *Cloud* public propose désormais aux entreprises des applications davantage spécialisées (allant de la gestion des forces de ventes à l'ERP en ligne). Ce type d'offres peut disposer d'une protection de l'accès aux données plus élaborée que le simple statut « privé » évoqué ci-dessus.

Enfin, une nouvelle sous-catégorie de *Cloud* public voit le jour avec le projet français de *Cloud* souverain, Andromède, qui a donné lieu à la création de deux sociétés : *Cloud*Watt (Orange et Thales) et Numergy (SFR et Bull) en France. Il s'agit de proposer une offre *Cloud* dont l'infrastructure est maîtrisée par un hébergeur national, voire européen, pour mieux répondre aux exigences de l'UE en termes de protection des données à caractère personnel, et de maîtrise des risques d'espionnage. Le *Cloud* souverain limite en partie ces risques, mais n'offre pas, pour autant, l'assurance de les couvrir. L'analyse de risque devra donc obéir aux mêmes exigences que dans le cas d'un *Cloud* public.

Typologie des données

Pour protéger les données de façon adéquate, il est fondamental qu'elles soient inventoriées et qualifiées selon une typologie distinguant les données sensibles des autres données utilisées et traitées par le système d'information.

Pour qualifier les données, il existe de nombreuses méthodes, souvent lourdes à mettre en œuvre. Néanmoins, une méthode simple pour qualifier une donnée est d'évaluer quel serait l'impact pour l'entreprise si la donnée :

- était rendue indisponible,
- était utilisée ou modifiée par une personne non autorisée (interne ou externe),
- devenait publique ou largement diffusée.

et qu'il n'existait pas de surveillance efficace permettant de détecter cette perte de confidentialité, d'intégrité et de disponibilité, et d'en déterminer la cause et l'origine.

Ainsi, les données de l'entreprise peuvent être réparties selon les trois catégories suivantes :

- les données sensibles à caractère personnel (cf. CNIL),
- les données stratégiques pour l'entreprise,
- les autres données utilisées dans les applications métiers.

Nous définissons les données stratégiques de l'entreprise comme un ensemble d'informations qui, si elles étaient détenues ou mises en corrélation par des tiers, pourraient permettre de prendre de vitesse ou neutraliser une prise de position envisagée par l'entreprise et dont l'impact serait d'une telle ampleur, que la stratégie de l'entreprise serait fortement ou durablement impactée.

Par ailleurs, le caractère stratégique d'une donnée est lié à la durée de validité de l'axe stratégique de l'entreprise (fusion, appel d'offres…) qu'elle concerne. Une donnée stratégique peut alors être confidentielle ou sensible pendant un temps déterminé, et perdre cette caractéristique ultérieurement.

Bonnes pratiques

Gouvernance de la protection des données

La protection des données n'est pas spécifiquement liée à l'émergence du *Cloud*. C'est une problématique ancienne et indispensable à la gestion de ces actifs informationnels et à la mise en conformité de l'entreprise avec le cadre législatif relatif à la protection des données. Néanmoins, la mise en œuvre d'une solution de *Cloud Computing* doit être l'occasion de mettre en place ou d'actualiser sa gouvernance de la protection des données.

Avant de se lancer dans un projet *Cloud*, les entreprises doivent être préalablement sensibilisées à la protection des données et avoir mis en place un programme d'entreprise sur ce sujet. La DSI est un acteur incontournable de cette bonne gouvernance, mais il n'est pas le seul. En effet, elle implique de nombreux acteurs à tous les niveaux, comme le montre l'exemple ci-dessous, que l'on pourra adapter en fonction des spécificités de l'entreprise.

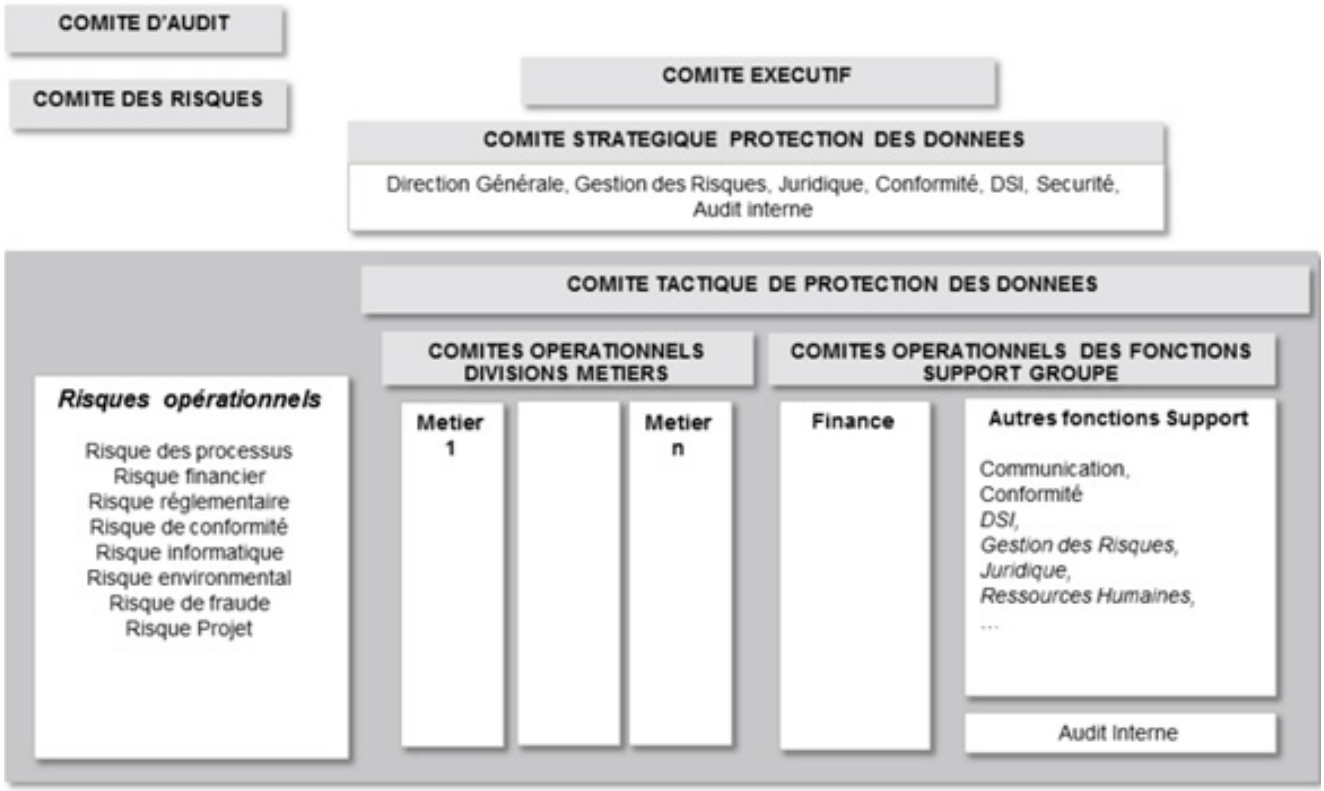

Figure 2 - Exemple d'organigramme d'un programme de protection des données
(Source ***Groupe de travail AFAI-CIGREF-IFACI 2013****)*

Comme tout dispositif de maîtrise des risques, la protection des données requiert :

- des objectifs clairs,
- le support du management,
- l'implication de toutes les parties prenantes (métiers et fonctions support groupe),
- une gouvernance (comités, rôles et responsabilités) appropriée,
- un plan d'action détaillé spécifiant les ressources et budget,
- un suivi du plan d'action.

Une implication responsable des **propriétaires des traitements et des données** est indispensable en matière :

- d'identification et d'évaluation des risques,
- de qualification des données,
- de gestion des autorisations d'accès aux applications,
- de conception, de mise en œuvre, de test et de suivi de l'efficacité des contrôles associés.

La DSI est, quant à elle, impliquée dans la sécurisation :

- des applications,
- des bases de données et des systèmes,
- du réseau,
- des infrastructures,
- de la conception, de la mise en œuvre et du suivi de l'efficacité des contrôles.

L'audit interne contribue à la maîtrise de l'usage du *Cloud* en évaluant notamment :

- le processus de sélection,
- le référentiel de contrôle du prestataire,
- la gouvernance de la prestation, y compris par l'exécution de la clause contractuelle d'audit.

Questions à se poser avant de souscrire une offre *Cloud*

Avant de mettre en place une solution *Cloud* dans l'entreprise, il est nécessaire de répondre aux questions suivantes.

◆ Quels sont les traitements et les données susceptibles de migrer vers le *Cloud* ?

La première question à se poser avant de souscrire une offre concerne l'identification des données qui seront hébergées dans le *Cloud* et de leur traitement. Certains types de données sont en effet soumis à des exigences réglementaires ou Métiers particulières, qu'il faut alors identifier avant de valider leur transfert dans le *Cloud*.

Il est important de ne pas faire de choix ponctuel, dicté uniquement par des considérations informatiques. Le choix doit être effectué à partir des services que l'on veut offrir aux utilisateurs :

- décrire au préalable le processus Métier de bout en bout, pour s'assurer de la continuité opérationnelle, vue par les utilisateurs,
- identifier les interfaces entre les SI internes et les futurs SI hébergés sur le *Cloud*, le chemin critique, les éventuelles ruptures de charge dans le flux des données,
- vérifier la cohérence de fonctionnement entre les SI internes et ceux qui seront hébergés sur le *Cloud* (temps de cycle, points de reprises en cas d'anomalies, gestion des changements, gestion des incidents…).

◆ Quelles sont les opportunités du *Cloud* par rapport à une informatique « traditionnelle » ?

Pour une entreprise, les opportunités potentielles du *Cloud*, par rapport à une informatique plus traditionnelle, sont entre autres :

- une meilleure flexibilité et évolutivité, par la mise à disposition réactive des services et l'adaptation en continu, au niveau des besoins ;
- un accès rapide aux dernières technologies et sans nécessité d'investir en moyens et en compétences supplémentaires ;
- une baisse des coûts, à confirmer néanmoins de manière spécifique et systématique, issue de la mutualisation des infrastructures, la standardisation et la banalisation des applications : les dépenses d'investissements sont réduites et remplacées par un coût à l'usage, au juste nécessaire (selon une enquête réalisée en 2011 par la Commission européenne [1], le *Cloud* permettrait à 80% des entreprises de réduire leurs coûts de 10% à 20%) ; pour des projets mal préparés ou mal suivis, le coût pourra être supérieur à d'autres solutions classiques.

◆ Quels sont les risques à maîtriser ?

Les principaux risques inhérents à la mise en œuvre d'une solution *Cloud* dans le SI de l'entreprise sont [2] :

- Perte de maîtrise des traitements :
  - perte de maitrise des normes et technologies mises en œuvre par le fournisseur ;
  - difficultés d'intégration entre services disponibles en interne et ceux qui sont sur le *Cloud*, ou entre diverses briques *Cloud* de fournisseurs différents ;
- Dépendance technologique et fonctionnelle vis-à-vis du fournisseur de *Cloud* et difficulté pour exercer la réversibilité du fait d'une perte de compétences SI et fonctionnelles en interne ;

[1] Source : *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : «* Unleashing the Potential of Cloud Computing in Europe *»*, page 4

[2] Source CNIL

- Faille dans la sécurité des données :

  - disponibilité : perte de maitrise du système d'information et manque de visibilité sur les dysfonctionnements ;
  - intégrité : risque de perte de données, de destruction, d'altération par erreur ou malveillance ;
  - confidentialité : risque d'intrusion, d'usurpation ou de non étanchéité entre les différents utilisateurs ;
  - traçabilité difficile ou impossible des données et des accès ;
  - problème de gestion des droits d'accès…

- Non maîtrise de la localisation des données et des intervenants ;
- Incapacité pour le client de répondre en temps et en heure aux requêtes judiciaires ;
- Réquisitions judiciaires imposées aux prestataires selon les juridictions compétentes entraînant une perte de confidentialité et/ou de disponibilité des données pour le client ;
- Non-conformité réglementaire, notamment sur les transferts internationaux ;
- Destruction ineffective ou non sécurisée des données, ou durée de conservation trop longue, au-delà des délais légaux de conservation (sauvegardes, archives…) ;
- Sauvegarde ineffective ;
- Incapacité du client à modifier l'application en cas d'évolution de ses besoins fonctionnels ;
- Faille dans la chaîne de sous-traitance impactant le niveau de service ;
- Indisponibilité du service du prestataire ;
- Difficulté à tester et à mettre en œuvre un Plan de Continuité d'Activité métier (BCP) cohérent avec le DRP (*Disaster Recovery Plan*) du fournisseur ;
- Cessation d'activité du prestataire ou acquisition du prestataire par un tiers.

Une analyse de risques permet d'identifier les mesures de sécurité complémentaires à mettre en place dans l'entreprise au moment de la souscription de l'offre *Cloud*. Ces mesures peuvent concerner l'entreprise comme le prestataire choisi (cf. page 17 § Quel impact sur la politique de sécurité interne ?).

◆ Quel *Cloud* pour quel traitement ?

Toutes les solutions de *Cloud Computing* ne sont pas adaptées à tous les types de données et de traitements dans l'entreprise.
Le choix du modèle privé ou public, voire partagé, interconnectant environnements externes et internes à l'entreprise doit prendre en compte, selon Gartner, plusieurs paramètres :

- Le calcul des coûts d'exploitation à court et moyen terme,
- Le niveau de flexibilité recherché,
- Les besoins de consacrer les ressources internes sur des activités à forte valeur ajoutée, favorable à l'innovation,

- Les contraintes des charges de travail,
- La sécurité,
- La qualité de services et la souplesse contractuelle vis-à-vis des fournisseurs
- La performance et la disponibilité,

Le tableau ci-dessous donne une première grille de sélection d'une catégorie de *Cloud* en fonction du type de données qui y sera hébergé :

Type de donnée sensible	**Catégorie de *Cloud***		
	Externe - Ouvert	Externe - Privé	Interne - Privé
Stratégique			
Personnelle			
Métier			

Usage inadapté de la catégorie de *Cloud* pour le type de données concerné

Usage à déterminer en fonction des résultats de l'analyse de risques

Usage adapté de la catégorie de *Cloud* pour le type de données concerné

◆ Comment choisir le prestataire ?

La plupart des offres *Cloud* proposées sur le marché sont « standard ». L'entreprise doit donc évaluer si les offres envisagées répondent aux exigences de sécurité préalablement définies en interne :

- Si l'entreprise dispose d'un cadre de contrôle interne relatif à la protection de données, elle doit le communiquer au prestataire,
- En l'absence d'un tel référentiel, elle peut s'appuyer sur des questionnaires d'évaluation fournis par des organismes de normalisation reconnus (voir exemples en annexe) ou sur des certifications (ISO 27001) et /ou des attestations (ISAE3402, SOC 1 & 2, …).

Le prestataire doit être capable d'apporter des garanties suffisantes notamment sur les mesures de sécurité et de confidentialité appropriées. Il doit également être transparent par rapport aux moyens employés.

Lors du choix du prestataire, il est primordial de :

- Déterminer la qualification juridique de la prestation, sachant que le prestataire peut être conjointement responsable du traitement en s'interrogeant sur :
  - la juridiction de référence,
  - la collecte des données,
  - l'usage des données
- S'assurer de la localisation des données

• Evaluer le niveau de protection que le prestataire assure aux données traitées (confidentialité, intégrité, disponibilité, traçabilité) :

- par une exploitation sécurisée et efficace : sécurisation physique des locaux, sécurisation de l'infrastructure technique, gestion des incidents, gestion des changements, gestion et sauvegarde de la configuration, tests de sécurité, chiffrement des communications, journaux, redondance des moyens, gestion des identités, gestion des accès distants, procédures de surveillance et d'audit…
- par une confirmation de la localisation des données,
- par un personnel formé et expérimenté (politique d'embauche, de formation, encadrement des accès privilégiés, recours à des sous-traitants ou à des tiers…),
- par une définition explicite des niveaux de service (SLA, pilotage, support et assistance, escalade…),
- par l'assurance de la localisation des opérateurs.

Il faut également vérifier la possibilité d'exporter ses données (avec effacement total) afin de ne pas se retrouver ensuite dépendant de ce fournisseur.

L'établissement d'un Plan d'Assurance Sécurité [1] (PAS) approprié pourra être requis en fonction de la criticité des données, telle que définie dans l'analyse de risques.

◆ Quel impact sur la politique de sécurité interne ?

Les problèmes de sécurité générés par le *Cloud* sont ceux déjà rencontrés dans l'utilisation quotidienne d'Internet par les entreprises, en particulier le problème de la confidentialité des échanges. Le passage au *Cloud computing* met en évidence, voire amplifie, les failles de sécurité préexistantes en local.

Avant tout déploiement de SI basé sur le *Cloud*, le client doit disposer d'une infrastructure saine et fonctionnelle : vérifier et optimiser la sécurisation de ses données, de son infrastructure et de son réseau avant de passer au *Cloud* (antivirus, antispywares, monitoring réseau…). Il faut également faire évoluer les procédures, notamment en ce qui concerne les accès.

Recommandations contractuelles relatives à la protection des données

L'entreprise doit définir des critères de choix du prestataire à partir de l'analyse de risques : « quel niveau de service pour quelles données ? ».

Idéalement, le projet ne doit démarrer qu'une fois le contrat signé. Dans la pratique, la finalisation contractuelle, qui est souvent une opération longue, peut s'achever après le démarrage du projet.

[1] Source : « Maîtriser les risques d'infogérance » - Chapitre 4 : Le plan d'assurance sécurité - ANSSI 2010

Dans ce cas, il est important d'intégrer dès la lettre d'intention une clause suspensive si les critères de protection des données requis ne sont pas atteints.

Au-delà des critères techniques mis en place par le fournisseur de service *Cloud*, il est primordial d'intégrer dans les clauses contractuelles des obligations fortes en matière de disponibilité, d'intégrité, de confidentialité, d'audit et de conformité exigées par l'entreprise, ses clients et les régulateurs.

Le cadre contractuel doit être validé par le département juridique, éventuellement assisté d'experts juridiques en matière de protection des données, afin d'engager la responsabilité du fournisseur, qui en cas de non-respect doit être soumis à des pénalités financières.

Le fournisseur devra pouvoir démontrer qu'il a mis en œuvre les mesures de sécurité adéquates par rapport au référentiel de contrôle du client.

◆ Disponibilités des données ?

Pour se prémunir contre le risque de perte de données, il est préconisé de répliquer celles-ci sur un autre site distant et d'exiger un engagement de résultat de restauration des données dans des délais contractuels définis.

En cas de perte de données, le client doit être alerté et pouvoir enquêter.

◆ Intégrité et confidentialité des données ?

Les clauses de responsabilité du contrat doivent être clairement définies, tout particulièrement en matière de respect de la confidentialité des données (accès non autorisés, voire frauduleux), et d'atteinte à leur intégrité. Dans certains cas, comme par exemple, dans le domaine médical ou de la défense nationale, le client pourra exiger que :

- ces données restent localisées sur des serveurs exclusivement situés dans l'UE,
- le prestataire soit français et/ou agréé par l'Etat,
- les moyens de contrôle de cette obligation lui soient fournis par son prestataire.

Avec un stockage et un accès aux données personnelles à l'intérieur de l'UE, le client s'exonérera ainsi d'un ensemble de formalités CNIL liées au transfert de données en dehors de l'UE.

Dans le domaine médical, le prestataire doit se conformer à un cahier des charges strict qui donne lieu à des audits réguliers et à un agrément par le Ministère de la Santé, valide pendant 3 ans.

Dans le cadre d'un service *Cloud* qui héberge des données à caractère personnel, géré par des opérateurs *offshore* (hors UE), il est nécessaire de s'assurer que l'on est en conformité avec les règlements relatifs aux transferts internationaux de données. Ceci est notamment vrai même si les données restent physiquement en Europe, mais que le personnel qui y accède se trouve en dehors de l'Europe.

Pour ce faire, le client et son prestataire peuvent recourir à l'un des mécanismes ci-dessous :

- déclaration de transferts internationaux entre le contrôleur (propriétaire de données) et le processeur (fournisseur de service),
- *Binding Corporate Rules*[1],
- clauses contractuelles européennes (*Standard Clauses*[2]).

Il est à noter que certains pays sont exemptés de tels dispositifs :

- les États membres de l'UE : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie, la Slovénie et la Suède,
- les Etats membres de l'EEA : l'Islande, le Liechtenstein et la Norvège,
- les autres pays exemptés : Andorre, Argentine, Australie, Canada, Guernesey, Ile de Man, Iles Féroé, Israël, Monaco, Suisse.

◆ Convention de niveau de services - SLA *(Service Level Agreement)*

Une convention de niveau de service de sécurité doit être contractuellement définie avec le prestataire en fonction du niveau de protection requis pour la catégorie de données concernée et traiter notamment les incidents, la confidentialité, l'intégrité, la disponibilité, la traçabilité, les performances, les vulnérabilités.

La rédaction de cette convention de niveau de services peut s'inspirer du document de l'ANSSI : « Maîtriser les risques d'infogérance » - Chapitre 4 : Le plan d'assurance sécurité.

Le prestataire doit disposer d'outils de mesure, d'indicateurs du niveau de « service sécurité » et rendre compte de ces mesures au client. Un système de malus ou de pénalités pourrait être appliqué en cas de non-respect de la convention.

Dans le cas d'un service *Cloud* nécessitant un niveau de protection élevé, cette convention est une condition *sine qua non*.

◆ Clause d'audit

Le prestataire de services de *Cloud Computing* doit intégrer dans son offre, un audit annuel par une société indépendante et/ou autoriser le client à organiser lui-même des audits ; le prestataire doit s'engager à traiter les déficiences observées. Attention, l'absence de clause d'audit dans le contrat peut rendre toute mission commanditée par le client non recevable.

Un exemple de clause d'audit est disponible en annexe 3.

[1] Voir Annexe 2 : Normes, Certifications

[2] Voir Annexe 2 : Normes, Certifications

◆ Plan de réversibilité

Pour assurer une pérennité des services de *Cloud*, il s'avère primordial de contractualiser un plan de réversibilité permettant de transférer les services à d'autres prestataires ou de les réintégrer dans l'entreprise. Ce plan prévoira notamment les facteurs déclencheurs de cette réversibilité (carence du prestataire, libre choix du client à échéance du contrat après un certain nombre d'années…), les conditions de cette réversibilité (simple discontinuité du service, arrêt total du service…) et le coût de celle-ci pour l'entreprise.

La mise en œuvre de la réversibilité devra inclure la suppression des données par le prestataire sur ses moyens propres.

Mise en œuvre et pilotage de la protection des données

Pour assurer le respect des engagements contractuels, le client doit disposer de moyens de pilotage et de suivi opérationnel.

Le prestataire de services *Cloud* doit être en mesure de fournir des éléments de preuve suffisants à son client, à travers un dispositif de contrôle efficace et testé par des auditeurs indépendants. Le prestataire doit pouvoir communiquer ces éléments aux acteurs concernés (la direction, les auditeurs internes, les clients ou les régulateurs) et démontrer ainsi que le niveau de protection des données est satisfaisant.

Cette démonstration peut se concrétiser par la publication de « Rapports d'assurance » de type ISAE 3402.

◆ Structurer la gouvernance de la prestation

Dans la phase de mise en œuvre, il est nécessaire de déployer une gouvernance avec des responsabilités clairement définies et suivies lors de réunions du comité de pilotage. Les questions relatives à la protection des données doivent être plus spécifiquement suivies par un comité de sécurité.

Un comité de sécurité régulier doit être mis en place entre le client et le prestataire, et animé par les correspondants sécurité des deux parties pour traiter des sujets suivants :

- la conformité des services de sécurité (patchs sécurité, anti-virus…),
- la gestion du risque opérationnel (identification, évaluation, remédiation) et le suivi des actions de remédiation des vulnérabilités critiques identifiées,
- les incidents, les intrusions et leur traitement,
- la gestion des contrôles, des audits et des rapports d'assurance (planification, périmètre, certification).

◆ Définir et mettre en place les mesures de protection exigées

• *Périmètre des contrôles par rapport aux services fournis*

Le client doit vérifier que le périmètre de contrôle du prestataire couvre bien le service demandé. Il est possible, par exemple, que le prestataire n'ait mis en œuvre qu'un sous-ensemble des activités de contrôle attendues.

A titre d'exemple, un prestataire peut avoir mis en œuvre des activités de contrôle en matière de sécurité physique et environnementale, ainsi qu'en matière de sécurité réseau mais très peu en matière de sécurité logique, parce que le prestataire avait historiquement un métier d'hébergeur (IaaS) et a peu de maturité en matière de service logiciel (SaaS). Dans ce cas, le prestataire disposera d'un rapport, qui est un gage de sécurité physique, mais qui ne couvre pas les activités de contrôle liées aux accès logiques.

• *Objectifs et activités de contrôle*

En matière de protection de données, on peut distinguer cinq familles d'objectifs de contrôle (détaillées dans l'annexe 1) :

1. les données sensibles : le prestataire doit mettre en œuvre, de façon cohérente, les processus en matière de sécurité, gestion du personnel, inventaire, qualification et traçabilité des données,
2. les *datacenters* : le prestataire doit disposer d'une gestion sécurisée des accès physiques aux datacenters,
3. la sécurité des accès logiques : le prestataire doit disposer de contrôles d'accès logiques assurant la protection des données,
4. la sécurité des systèmes : le prestataire doit disposer de systèmes correctement configurés et protégés des failles de sécurité, en particulier pour les environnements hébergeant les données,
5. la sécurité du réseau : le prestataire doit disposer d'un réseau sécurisé avec un isolement approprié des autres clients.

◆ Assurer le suivi de la prestation

Le suivi de la prestation implique que le client :

- suive et contrôle les indicateurs de niveau de service de sécurité transmis par le prestataire à l'occasion de chaque réunion du comité sécurité,
- analyse les rapports d'assurance du prestataire,
- active la clause d'audit (notamment la capacité du client à réaliser des tests d'intrusion permettant de mesurer la robustesse effective de la sécurité de la prestation) et l'organiser en coordination avec le prestataire.

Annexes

Annexe 1 : objectifs de contrôle

En matière de protection de données, on peut distinguer cinq familles de contrôle :

1. les données sensibles : le prestataire doit mettre en œuvre, de façon cohérente, les processus en matière de sécurité, gestion du personnel, inventaire, qualification et traçabilité des données,

2. les *datacenters* : le prestataire doit disposer d'une gestion sécurisée des accès physiques aux datacenters,

3. la sécurité des accès logiques : le prestataire doit disposer de contrôles d'accès logiques assurant la protection des données sensibles,

4. la sécurité des systèmes : le prestataire doit disposer de systèmes correctement configurés et protégés des failles de sécurité, en particulier pour les environnements hébergeant les données sensibles,

5. la sécurité du réseau : le prestataire doit disposer d'un réseau sécurisé avec une isolation appropriée des autres clients.

Pour chacun de ces objectifs, des activités de contrôle doivent être réalisées.

A titre d'exemple, sont listées ci-dessous des activités de contrôle pour chacun de ces objectifs.

• Données

Le prestataire assure que :

- la localisation des données sensibles du client est connue et conforme aux exigences du client (*datacenter* et serveur),
- les systèmes de sauvegardes et plans de secours informatiques associés sont mis en œuvre,
- il dispose d'un code d'éthique appliqué par son personnel et il n'exerce pas des activités pouvant entrainer un risque de conflits d'intérêt,
- son personnel suit régulièrement des formations de sensibilisation à la sécurité,
- il dispose de moyens de traçabilité centralisés permettant de détecter des violations de privilèges ou des comportements malveillants,
- il dispose d'une gestion des incidents de sécurité incluant la détection, l'alerte, le traitement jusqu'à la résolution, l'identification des causes et la communication au client.

• ***Sécurité des accès physiques***

Le prestataire assure que :

- il dispose de systèmes d'accès physique sécurisés, de détection d'intrusion et de vidéo surveillance,
- les accès aux *datacenters* sont autorisés aux seules personnes habilitées en suivant un circuit d'approbation approprié, ils sont tracés et revus régulièrement,
- tout sous-traitant de maintenance amené à utiliser ou réparer des équipements contenant des données sensibles est soumis à des clauses contractuelles de confidentialité,
- tout media de stockage de données contenant des données sensibles et destiné à être mis au rebus ou recyclé fait l'objet d'un effacement physique préalable de ces données.

• ***Sécurité des accès logiques***

Le prestataire assure que :

- il applique les règles d'autorisation d'accès aux données en fonction des éléments communiqués par le client (création, modification et suppression) ; il fournit la liste des accès au client,
- les accès des utilisateurs et administrateurs aux systèmes contenant des données sensibles s'appuient sur des mécanismes assurant la confidentialité et la traçabilité (pistes d'audit sur les accès aux données et traitement de la problématique des comptes génériques),
- il applique une politique d'authentification et de mot de passe conforme à celle du client.

• ***Sécurité des systèmes***

Le prestataire assure que :

- les données sauvegardées quel que soit le support sont chiffrées,
- il gère les vulnérabilités des systèmes et organise au moins annuellement des tests d'intrusion ; les vulnérabilités critiques identifiées sont corrigées immédiatement,
- les serveurs hébergeant des données sensibles sont configurés avec un niveau de sécurité renforcé ; les patchs de sécurité sont gérés de façon centralisée et appliqués dans des délais inférieurs à un mois,
- les anti-virus sont installés sur les serveurs, mis à jour et supervisés,
- l'usage des clés USB ou autres media de stockage mobile est contrôlé et interdit sur tous les systèmes contenant des données sensibles.

• ***Sécurité des accès au réseau***

Le prestataire assure que :

- les points d'entrée au réseau sont limités, sécurisés et filtrés,
- les tâches d'administration des systèmes sont opérées depuis un réseau d'administration dédié et isolé en se connectant avec des mécanismes d'authentification forte,
- les changements d'équipement réseau sont tracés, documentés et approuvés,
- dans le cas d'un *Cloud* partagé :

- l'accès au réseau est autorisé uniquement à des terminaux de confiance,

- le réseau sur lequel sont connectés les systèmes hébergeant les données sensibles est isolé du réseau des autres clients.

Annexe 2 : normes, certifications

◆ Certifications

• ***AUP (Agreed Upon Procedure)***

Les revues AUP (*AGREED UPON PROCEDURES*) sont utilisées quand un client demande à un auditeur externe d'effectuer des tests sur des procédures spécifiques et d'établir un rapport sur les résultats.

Dans le rapport, l'auditeur ne fournit aucune opinion, certification, ou assurance que les affirmations faites sont exemptes d'anomalies significatives. Les destinataires de ce type de rapport doivent tirer leurs propres conclusions sur les résultats des tests réalisés. Par exemple, un auditeur externe sera amené à demander des pièces justificatives prouvant l'application d'une procédure ; il fera état de la sélection de ces pièces et du résultat de ces tests, mais ne donnera pas un avis formel avec des conclusions sur leurs résultats.

• ***ISAE3402 type I et type II (ex-SAS70)***

L'externalisation d'une activité nécessite de maîtriser les risques car elle a un impact direct sur les comptes des entreprises et sur leurs informations financières. Les entreprises doivent donc contrôler que leurs prestataires (du service externalisé ou le sous-traitant) ont mis en place des procédures conformes à leurs exigences.

Conséquence : les prestataires subissent donc une hausse de demandes d'information et d'audit de la part de leurs nombreux clients. Une solution alternative à des audits commandités par chaque client est donc envisagée : une attestation émise par un tiers indépendant sur la qualité de leur dispositif de contrôle interne. Elle prévoit la transmission de rapports sur la qualité des procédures de contrôle interne d'un prestataire à l'intention de l'entreprise cliente.

Les prestataires concernés doivent généralement réaliser des travaux en vue d'éliminer les défauts de leurs procédures de contrôle interne et de rendre ces dernières exhaustives et homogènes. Au final, le rapport ISAE3402 renforce la crédibilité des prestataires vis-à-vis de leurs clients.

Le recours à cette norme doit s'inscrire dans un processus comprenant plusieurs étapes. Le prestataire concerné doit d'abord formaliser précisément son dispositif de contrôle interne, ses objectifs de contrôle et les contrôles liés, puis établir un document décrivant l'ensemble de ce dispositif. C'est sur la base de ce document que le vérificateur, en règle générale un cabinet d'audit, exprimera une opinion.

En pratique, il existe deux types de rapports :

- un rapport de type I, dans lequel le vérificateur émet une opinion sur la fidélité de la description et sur l'adéquation des contrôles par rapport aux objectifs fixés. Ce type de contrôle s'effectue une fois par an. Les entreprises utilisent généralement ce premier rapport pour déterminer une tendance avant d'aller vers le rapport de type II. Cette certification a comme inconvénient de ne décrire l'organisation qu'à un temps T et non sur une période,

- un rapport de type II, plus complet du fait d'une étude portée sur une période (de 6 mois minimum en général), dans lequel le vérificateur émet en plus une opinion sur l'efficacité des contrôles pour atteindre ces objectifs. L'attestation ISAE3402 de type II est donc l'attestation la plus complète. Elle intègre non seulement un audit au moment de l'attestation, mais ensuite des contrôles réguliers pour s'assurer que les procédures mises en place restent bien appliquées. Elle constitue une opportunité supplémentaire pour l'entreprise d'améliorer sans relâche son organisation. Pour chaque service audité, une grille de contrôle a été mise en place avec une liste des objectifs de contrôle, des activités contrôlées, des plans de test, des observations et recommandations.

• *SOC 2 et SOC 3*

L'American Institute of Certified Public Accountants (AICPA) a aussi défini les rapports des *Service Organization Controls* (contrôles des fournisseurs de services) - SOC2 et SOC3.

- SOC 2 est un rapport sur les contrôles d'un organisme de services touchant à la sécurité, la disponibilité, la confidentialité de traitement d'intégrité, de confidentialité, et/ou utilisant des critères prédéfinis et couvrant un ou plusieurs des cinq attributs clés du système de sécurité, de disponibilité, d'intégrité du traitement, de confidentialité et de vie privée. La diffusion du rapport SOC 2 se limite aux clients de l'entreprise de services et à des destinataires bien spécifiques qui ont une connaissance approfondie de l'organisation du service et de ses contrôles internes.

- SOC 3 est un rapport qui utilise les mêmes attributs que le SOC 2. Le SOC 3 est un rapport d'utilisation générale qui ne fournit que le rapport du vérificateur si le système a atteint les critères de base des services, laissant de côté le système et des descriptions détaillées de test.

- ***Unified Certification Standard™ (UCS) for Cloud & Managed Service Providers***

L'UCS, précédemment connu sous le nom de *Managed Services Accreditation Program* (MSAP), dispose d'auditeurs qui visitent les installations des fournisseurs de services *Cloud*, et les évaluent sur onze objectifs de contrôle principaux.

- ***Code of Practice for Cloud Service Providers Self Certification***

Les organisations garantissant le respect du *Code of practice* défini par le Cloud Industry Forum (CIF) procèdent à une auto-certification annuelle et confirment les résultats positifs de cette attestation au CIF afin de recevoir l'autorisation d'utiliser la marque de certification (le «logo») pour l'année suivante.

- ***EuroCloud Star Audit Certification***

EuroCloud Allemagne a lancé un programme de certification pour les solutions et technologies SaaS/*Cloud*. Il est en cours de déploiement au niveau européen. L'évaluation est faite par un tiers agréé, et prend la forme de l'attribution d'un nombre d'étoiles.

Ce programme de certification (disponible en anglais uniquement) couvre les points suivants :

- Conformité réglementaire,
- Sécurité et confidentialité des données,
- Infrastructure des datacenters,
- Processus opérationnels,
- Interopérabilité et implémentation des applications.

- ***CSA Open Certification Framework***

Le *Cloud Security Alliance* (CSA) a créé l'*Open Certificate Framework* (OCF) en partenariat avec le BSI (British Standards Institution). Ce partenariat s'assurera que l'*Open Certificate Framework* est en conformité avec les normes internationales et est basé sur un processus complet de certification.

L'*Open Certificate Framework* est structuré en trois niveaux, et chacun d'entre eux offrira un niveau supplémentaire de confiance et de transparence aux activités des fournisseurs de services du *Cloud* et un niveau plus élevé d'assurance pour le consommateur *Cloud*.

- Le niveau initial est l'auto-évaluation CSA STAR : les fournisseurs de *Cloud* peuvent envoyer des rapports au Registre STAR CSA pour indiquer leur conformité avec les meilleures pratiques du CSA. La disponibilité est immédiate.

- Le deuxième niveau, la CERTIFICATION CSA STAR, est une évaluation par un tiers indépendant : cette certification s'appuie sur les exigences de la norme ISO/IEC 27001 : 2005 avec la matrice CSA *Cloud Control* (CCM). Ces évaluations seront menées par des organismes de certification approuvés seulement. La disponibilité est prévue au 1er semestre 2013.

- La certification STAR sera renforcée à l'avenir par une surveillance continue basée sur la certification : ce troisième niveau est actuellement en cours de développement.

• *ISO/IEC 27001*

La certification ISO 27001 constitue la principale norme internationale servant à évaluer les systèmes de gestion de la sécurité des informations. Elle définit des exigences et meilleures pratiques pour une approche méthodique de la gestion des informations des entreprises et des particuliers. Elle repose sur des estimations périodiques des risques, adaptées aux menaces en perpétuelle évolution.

• *FEDRamp*

Le *Federal Risk and Authorization Management Program* (FedRAMP) *Service Mark* (SM) certifie qu'un fournisseur de *Cloud* a fait l'objet d'un processus rigoureux d'évaluation de la sécurité, en accord avec le *Federal Information Security Management Act* (FISMA) et en utilisant les contrôles définis dans la NIST Special Publication 800-53, Revision 4 « *Security and Privacy Controls for Federal Information Systems and Organizations* ». Cette évaluation doit être validée par un tiers, afin de vérifier que les contrôles sont testés et intégrés, et qu'ils respectent le périmètre de l'évaluation.

• *PCI/DSS*

Pour renforcer la sécurité des systèmes d'information, le *Payment Card Industry* (PCI) *Security Standards Council* a développé le PCI *Data Security Standard* (PCI DSS). Le standard PCI DSS liste un ensemble de points de contrôles relatifs aux systèmes d'information qui capturent, transportent, stockent et traitent des données de cartes bancaires. Les points de contrôles sont relatifs à des techniques informatiques, mais également à des procédures et à des contrôles organisationnels sur ces systèmes.

La conformité à PCI DSS permet de vérifier que les points de contrôles sont bien mis en œuvre et qu'ils sont efficaces pour la protection des données de cartes bancaires. Cette conformité passe, selon la taille de l'entreprise, par un audit effectué par un auditeur agréé ou par un questionnaire d'auto-évaluation à remplir par l'acteur concerné et à transmettre à sa banque. Cette conformité doit être vérifiée annuellement ainsi que par des tests techniques validant la bonne protection du site de l'acteur.

- ***TRUSTed Cloud Data Privacy Certification***

TRUSTed est le principal fournisseur de solutions pour la protection de la vie privée en ligne et fournit une gamme de services pour aider les entreprises à gagner la confiance de leurs clients et augmenter l'adhésion sur tous leurs canaux numériques : sites Web, applications mobiles, publicité, services « *in-the-Cloud* », statistiques d'entreprise ou email marketing.

TRUSTed Cloud Data Privacy certification est basée sur une norme de conformité pour des pratiques commerciales relatives à la collecte et l'utilisation des données définie par TRUSTed. Pour obtenir la certification, une entreprise doit fournir la preuve de ses pratiques de gouvernance de la vie privée et des données, pour les données collectées pour le compte d'utilisateurs, clients et partenaires.

◆ Organisations internationales

- ***ISACA***

L'ISACA est un organisme indépendant développant des normes et bonnes pratiques en matière de gouvernance, contrôle, sécurité, audit et assurance des Systèmes d'Information. L'AFAI est le chapitre français de l'ISACA.

L'ISACA a notamment développé les référentiels COBIT, Val IT, BMIS et Risk IT et délivre des certifications pour les professionnels des systèmes d'information : CISA, CISM, CGEIT and CRISC.

Les principaux référentiels de l'ISACA concernant la sécurité sont BMIS (*Business Model for Information Security*) et COBIT 5 for Information Security publié récemment. L'ISACA a également publié plusieurs guides et recueils de bonnes pratiques concernant le *Cloud Computing*.

- ***IIA***

L'IIA est l'association professionnelle internationale de l'audit interne représentée en France par l'IFACI. Elle élabore des normes et diffuse des bonnes pratiques d'évaluation des dispositifs de contrôle interne et de gestion des risques, dont des guides d'audit des technologies de l'information (GTAG). Elle promeut le professionnalisme des auditeurs internes à travers un code de déontologie, et des certifications professionnelles (CIA, CRMA).

• *NIST*

Le NIST (*National Institute of Standards and Technology*) est une organisation rattachée au Ministère du Commerce américain. Le NIST a élaboré le NIST 800 Series, qui est un ensemble de documents décrivant les procédures et les lignes directrices relatives à la sécurité des systèmes d'information du gouvernement américain.

Ces documents, librement téléchargeables, servent de base aux différentes institutions, privées comme publiques.

• *ENISA*

L'ENISA est l'agence européenne chargée de la sécurité des réseaux et de l'information. Elle a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit de différentes façons en :

- intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes,
- favorisant l'échange des meilleures pratiques,
- facilitant les contacts entre les institutions (nationales et européennes) et les entreprises.

L'ENISA, en collaboration avec les instances nationales et les institutions européennes, s'emploie à développer une culture de la sécurité des réseaux d'information dans toute l'Union européenne.

• *Shared Assessments*

Shared Assessments a été créé par des institutions financières de premier ordre, les « Big 4 » des cabinets d'audit, ainsi que par des sociétés de services clés, pour apporter standardisation, consistance, vitesse, efficience et réduction de coûts dans le processus d'évaluation des risques des fournisseurs. A travers l'adhésion au *Shared Assessments Member Forum et l'utilisation des Shared Assessments Tools* (les *Agreed Upon Procedures et le questionnaire Standard Information Gathering*), *Shared Assessments* procure les moyens de conduire une évaluation rigoureuse et compréhensible des risques, de la sécurité et de la continuité des affaires.

◆ Organisations nationales françaises

• *CNIL*

La Commission Nationale de l'Informatique et des Libertés (CNIL) est une institution indépendante chargée de veiller au respect de l'identité humaine, de la vie privée et des libertés dans un monde numérique.

• ***ANSSI***

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est rattachée au Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. Elle a notamment pour mission de :

- détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques,
- prévenir la menace, en contribuant au développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques,
- jouer un rôle de conseil et de soutien aux administrations et aux opérateurs d'importance vitale,
- informer régulièrement le public sur les menaces, notamment par le biais du site internet gouvernemental de la sécurité informatique, lancé en 2008, qui a vocation à être le portail Internet de référence en matière de sécurité des systèmes d'information,
- constituer un réservoir de compétences, destiné à apporter son expertise et son assistance technique aux administrations et aux opérateurs d'importance vitale,
- promouvoir les technologies, les systèmes et les savoir-faire nationaux ; elle contribue au développement de la confiance dans l'économie numérique.

◆ Cadre réglementaire sur le transfert de données

Certains pays, ayant un niveau de protection adéquat, ne nécessitent pas d'autorisation de transfert. Il s'agit :

- des États membres de l'UE : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie, la Slovénie et la Suède,
- des Etats membres de l'EEA : l'Islande, le Liechtenstein et la Norvège,
- des autres pays exemptés : Andorre, Argentine, Australie, Canada, Guernesey, Ile de Man, Iles Feroe, Israël, Monaco, Suisse.

Si l'entreprise ne se trouve pas dans l'un des cas ci-dessus, elle peut utiliser l'une des trois solutions suivantes, ou demander une autorisation spécifique à l'autorité de protection des données compétente.

• *Les Binding Corporate Rules (BCR)*

Les *Binding Corporate Rules* (BCR) constituent un code de conduite, définissant la politique d'une entreprise en matière de transferts de données. Les BCR permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe.

Leur mise en place représente un effort conséquent, et est encore loin d'être généralisée dans les entreprises.

• *Les clauses contractuelles types de l'UE relatives aux données personnelles*

Ces clauses sont des modèles de contrats de transfert adoptés par la Commission européenne. On distingue :

- les clauses contractuelles types encadrant les transferts de données personnelles entre deux responsables de traitement,
- les clauses contractuelles types encadrant les transferts de données personnelles entre un responsable de traitement et un sous-traitant.

Il existe des exceptions au principe d'interdiction de transferts, qui sont l'objet de limitations et d'une interprétation stricte. Ces exceptions sont prévues par la directive 95/46 CE du 24 octobre 1995, et à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978 :

- Soit la personne a consenti expressément au transfert de ses données personnelles,
- Soit le transfert s'avère nécessaire à l'une des conditions suivantes :

  - à la sauvegarde de la vie de cette personne,
  - à la sauvegarde de l'intérêt public et au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice,
  - à la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime,
  - à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures pré-contractuelles prises à la demande de celui-ci,
  - à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Les principes du Safe Harbour

Le *Safe Harbour* comprend un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001.

Les entreprises établies aux États-Unis adhèrent à ces principes auprès du Département du Commerce américain. Cette adhésion les autorise à recevoir des données en provenance de l'Union européenne.

◆ Demandes d'accès et réquisitions de données

Les autorités nationales peuvent demander à accéder aux données localisées sur leur territoire et les réquisitionner le cas échéant, en application de lois nationales telles que le *Patriot Act* aux Etats-Unis ou la future directive européenne (Com. 2012-10).

Annexe 3 : Exemple de clause d'audit

Le Prestataire et les services qu'il fournit pourront faire l'objet d'audits qui auront notamment pour but de vérifier :

a. le respect de la convention de niveau de services - SLA (*Service Level Agreement*) ;

b. que le Prestataire se conforme aux procédures et aux normes de sécurité définies à l'article XX ;

c. que le Prestataire respecte les obligations qui lui incombent en vertu de l'article XX ;

d. que les moyens et les procédures mis en œuvre par le prestataire sont conformes au plan de gestion des désengagements, comme indiqué à l'article XX ;

e. et s'assurer que l'ensemble des documents comptables obligatoires et des données à collecter en vertu des lois et règlements applicables existe, est mis à jour conformément aux méthodologies généralement admises et, d'une façon générale, selon des modalités et avec un niveau de détail suffisants pour justifier le calcul des charges liées aux services. Le Prestataire est tenu de conserver tous les documents et pièces justificatives nécessaires pendant la durée du contrat et, au-delà, pendant le délai prévu par les politiques du Client telles qu'elles ont été notifiées au Prestataire ou, à défaut, conformément aux dispositions du présent Contrat et des lois et règlements applicables, étant précisé que le délai retenu ne peut être inférieur à six (6) mois ;

f. et mener des investigations conjointes avec le Prestataire, ou identifier les cas présumés de fraude ou d'erreur comptable significative.

Ces audits sont effectués par le Client ou par un Tiers désigné à cet effet. Le droit d'audit conféré au Client couvre également les cas dans lesquels l'audit est demandé par un tiers, notamment par l'administration fiscale, les sociétés d'assurance, les organismes publics, les régulateurs et les clients du Client.

Toutefois, ce tiers ne saurait être un concurrent du Prestataire et doit posséder une expérience avérée. Le Client s'engage à confirmer au Prestataire, à sa demande, que l'auditeur a une obligation de confidentialité. L'auditeur devra se conformer aux règles de confidentialité et de sécurité applicables dans les locaux du Prestataire soumis à l'audit qui lui auront été communiquées préalablement.

Le Prestataire s'engage à assurer la disponibilité du personnel et des systèmes nécessaires pour faciliter l'audit. La mission ne doit pas perturber anormalement les prestations de services confiées au Prestataire. Le Client et ses auditeurs auront accès aux locaux ou aux données confidentielles du Prestataire, de ses Sociétés affiliées ou du Client, dès lors qu'ils sont utilisés pour exécuter les services.

Le Client ne bénéficie d'aucun accès :

- aux informations concernant les autres clients du Prestataire ni aux informations sans lien avec les services,
- aux sites ou locaux du Prestataire (ou aux parties de ces derniers) sans lien avec le Client ou les services,
- aux documents du Prestataire relatifs au calcul de ses frais généraux internes ou de sa rentabilité,
- aux rapports d'audit à usage interne du Prestataire. L'accès du Client aux sites ou aux locaux du Prestataire (s'il est justifié) est soumis aux règles de sécurité ainsi qu'aux contrôles et à la surveillance du Prestataire.

L'audit est effectué au maximum deux fois par an, sauf s'il est imposé par un tiers tel que les autorités légales, l'administration fiscale, les sociétés d'assurance, les organismes publics ou les régulateurs. Le Client s'engage à déployer des efforts raisonnables pour informer le Prestataire par un préavis de dix (10) jours ouvrables. Ce délai est ramené à deux (2) jours ouvrables si l'audit est demandé par un organisme public ou une autorité de tutelle, ou en cas d'urgence. En outre, le Client s'engage à informer le Prestataire du périmètre de l'Audit.

Si l'exercice de ces droits d'audit et d'inspection affecte la capacité du Prestataire à remplir les obligations mises à sa charge par le présent contrat, le Prestataire en informe le Client et s'engage à étudier avec celui-ci, à sa demande, les moyens d'éviter un tel impact. Si cet impact est significatif et si le Client décide néanmoins d'exercer ses droits d'audit et d'inspection, et sous réserve que le Prestataire n'ait ménagé aucun effort pour s'acquitter de ses obligations conformément au présent contrat malgré l'exercice du droit d'audit et d'inspection, le Prestataire est alors affranchi de ces obligations (et de toute responsabilité pour manquement à celles-ci) pour autant qu'elles soient affectées et pendant la durée de cet impact. Si l'exercice du droit d'audit entraîne des coûts significatifs pour le Prestataire, celui-ci en informe le Client et cette question est examinée par les parties.

Si l'audit met en évidence un manquement du Prestataire aux obligations mises à sa charge par le présent contrat ou par les règles de droit qui lui sont applicables en sa qualité de prestataire des Services, le Prestataire prend rapidement toutes les mesures nécessaires pour remédier à ce manquement. Les dispositions de la présente clause s'appliquent sans préjudice des autres droits conférés au Client le cas échéant par le présent contrat ou par le droit en vigueur.

Le Prestataire communiquera au Client, dans les meilleurs délais, une synthèse des résultats des audits réalisés par tout membre du Groupe du Prestataire, par des sous-traitants ou par leurs agents ou représentants (y compris les auditeurs internes ou externes), ou communiquera au Client, à sa demande, une synthèse concernant tout audit effectué par des autorités de tutelle ou organismes de certification, dès lors que ces audits mettent en évidence des circonstances qui sont liées au service et qui pourraient avoir une incidence défavorable sur la capacité de certains membres du groupe Prestataire ou sous-traitants à exécuter certains des services conformément au présent contrat ou à respecter le droit applicable au Prestataire, ou qui sont susceptibles d'avoir toute autre incidence négative sur un membre du groupe du Client.

Chacune des Parties supporte ses propres coûts dans le cadre des inspections ou des audits réalisés en vertu du présent article XX. Toutefois, il est convenu que le Prestataire prendra à sa charge les coûts raisonnables engagés par le Client aux fins d'un audit (y compris les honoraires raisonnables des auditeurs ou des experts-comptables) s'il s'avère, au vu des résultats de cet audit, que le montant facturé au Client au titre de la fourniture de certains services a été largement surestimé, ou que le Prestataire a commis un manquement significatif aux obligations mises à sa charge par le présent contrat, étant entendu que le Prestataire ne sera tenu de supporter les coûts raisonnables susmentionnés du Client uniquement si ces coûts se rapportent à la (aux) partie(s) de l'audit qui a (ont) mis en évidence la surestimation ou la non-conformité.

Bibliographie

Recommandations

• *Unleashing the Potential of Cloud Computing in Europe [communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions] / European Commission*. 2012.

• Synthèse des réponses à la consultation publique sur le *Cloud computing* lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL.
CNIL, 2012.

• Recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud computing* / CNIL. 2012.

Ouvrages / Publications

• *Auditing Outsourced Functions: Risk Management in an Outsourced World / Mark Salamasick /* IIA, 2012.

• Guide d'hygiène informatique : quelques recommandations simples [1] / Agence nationale de la sécurité des systèmes d'information. ANSSI, 2012

• Protection de l'information d'entreprise et *Cloud computing* / INHESJ, CIGREF. 2012.

• Principes directeurs pour l'adoption et l'utilisation du *Cloud computing* / ouv. col. ISACA, 2012.

• *Enterprise risk management for Cloud computing / Crowe Horwath*, et al. COSO, 2012.

• Principes directeurs pour l'adoption et l'utilisation du *Cloud computing* / ouv. col. ISACA, 2012.

• *Global Technology Audit Guide: Information technology outsourcing, 2nd ed. / Bradley C. Ames*, et al. IIA, 2012.

• *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take: final report. / David Bradshaw,* et al. IDC, 2012.

[1] Version 0.1 soumise à appel à commentaires jusqu'au 15 novembre 2012

• *Cloud computing market maturity: study results* / ouv. col. - *Cloud Security Alliance* ; ISACA, 2012.

• *Security Considerations for Cloud Computing* / ouv. col. ISACA, 2012.

• *Calculating Cloud ROI : from the customer perspective* / ouv. col. ISACA, 2012.

• Gouvernance du système d'information / ouv. col. AFAI ; IFACI ; CIGREF, 2011.

• SaaS dans le SI de l'entreprise - La vision des grandes entreprises / ouv. col. CIGREF, 2011.

• *IT Control Objectives for Cloud Computing: controls and assurance in the Cloud* / ouv. col. ISACA, 2011.

• *Cloud Computing* : Impact du *Cloud Computing* sur la fonction SI et son écosystème / Guillaume BOUDOT, Jérôme DEJARDIN, Stéphane ROUHIER. CIGREF, 2010.

• *Cloud Computing* Management Audit / Assurance Program / Norm Kelson. ISACA, 2010.

• *Global Technology Audit Guide : Information security governance* / Paul Love. IIA, 2010

• Maîtriser les risques de l'infogérance / Agence nationale de la sécurité des systèmes d'information. ANSSI, 2010.

• Position du CIGREF sur le *Cloud computing*. CIGREF, 2010.

• *Cloud Computing: Implementation, Management, and Security* / John W. Rittinghouse, James F. Ransome. Taylor & Francis Group ; CRC press , 2009.

• *Security Guidance for Critical Areas of Focus in Cloud Computing* V.3 - *Cloud* Security Alliance, 2011.

• *Cloud Computing* : avantages pour l'entreprise et perspectives de sécurité, de gouvernance et d'assurance / ouv. col. – ISACA, 2009.

• *Cloud Controls Matrix V.1.3 / Cloud Security Alliance*, 2012.

• *Top 10 Big Data Security and Privacy Challenges / Cloud Security Alliance*, 2012

• *Consensus Assessments Initiative Questionnaire V.1.1 / Cloud Security Alliance*, 2011.

• *Personal Data: The Emergence of a New Asset Class / World Economic Forum*, 2011.

• *Cloud* : Les fondamentaux vus par les Grandes entreprises, 2013
(à paraître)

Colloques / Conférences

• *The 2012 European Cloud computing conference : making the transition from Cloud friendly to Cloud active (21st march 2012)*

• *The perfect storm : threats end risks in the Cloud [Internal auditing European conference*, Madrid, 2011] / Ramsés Gallégo. 2011.

• Aspects juridiques du *Cloud computing* [conférence Sécurité de la virtualisation et du *Cloud computing*, 14 avril 2010, Paris] / Blandine Poidevin. CLUSIF, 2010.

• *Cloud computing* et sécurité [conférence Sécurité de la virtualisation et du *Cloud computing*, 14 avril 2010, Paris] / Pascal Sauliere. CLUSIF, 2010.

Articles

• *Cloud Storage - Bursting Through the Hype / Rico Barrasso, Matt Wallace*, in ISACA Journal, vol. 5, 2012.

• *Cloud Risk - 10 Principles and a Framework for Assessment* / David Vohradsky, in ISACA Journal, vol. 5, 2012.

• Les enjeux de l'informatique en nuage [dossier] / Sarah Belouezzane, in Le Monde du jeudi 12 avril 2012.

- Pour les entreprises, une évolution qui attire et inquiète à la fois
- Les centres de données, au cœur du système / Florence Puybareau
- Amazon, le pionnier / Sarah Belouezzane
- Un nouveau mode de consommation / Florence Puybareau
- « Dassault Systèmes ne participera pas au *Cloud* national » [entretien avec Bernard Charlès] / Florence Puybareau

• Alerte au « *Cloud computing* » / Eric Blot-Lefevre. in Expertises, mars 2012.

• *Securing Cloud-based applications : how enterprise sigle sign-on was implemented to drive value* / Michael Mendelsohn, et al, in ISACA Journal vol. 1, 2012.

• *IT Governance and the Cloud : Principles and Practice for Governing Adoption of Cloud Computing / Ron Speed*. in ISACA Journal, vol. 5, 2011.

• Le *Cloud computing* en cinq idées reçues, in Chef d'entreprise magazine hors-série, décembre 2011.

• *Adoption of new technologies outpacing efforts to control resulting security and other risks*. CAE Bulletin, Nov. 30, 2011.

• La sécurité dans le *Cloud* : Une Approche Fournisseur Basée sur les Risques / Christophe Auberger. inforisk du 21 novembre 2011.

• Le *Cloud Computing*, un atout précieux pour la gestion des risques et des assurances / Pascal Stopnicki. inforisk du 28 octobre 2011

• Le « *Cloud* » peine encore à convaincre les entreprises / Romain Gueugneau. Les Echos du 5 octobre 2011.

• L'informatique dans les nuages / Christine Garcia, Sylvie Sadones, in Audit & Contrôle internes de septembre 2011.

• *Governance in the Cloud* / Joseph Kirkpatrick, in ISACA Journal, vol. 5, 2011.

• Branchés sur l'avenir : progrès bien tangible ou concept abstrait ? Quoiqu'il en soit, l'infonuagique offre des avantages importants aux entreprises. / Dwayne Bragonier, in Camagazine de septembre 2011.

• *Auditing the Cloud* / Brad Ames, Frederick Brown, in *Internal auditor, august* 2011.

• *The Borderless Enterprise* / Neil Baker, in *Internal auditor, august* 2011.

• *Head in the Clouds* / Dennis McGuffie, in *Internal auditor, august* 2011.

• *Cloud computing risk assessment : a case study* / Sailesh Gadia. in ISACA Journal, vol. 4, 2011.

• *Every Silver Cloud Has a Dark Lining: A Primer on Cloud Computing, Regulatory and Data Security Risk* / Carl Cadregari, Alfonzo Cutaia, in ISACA Journal, vol. 3, 2011.

• *Cloud computing [slideshow]* / The IIA. in Internal auditor.

cigref
Réseau
de Grandes Entreprises

ifaci
institut français de l'audit et du contrôle internes

AFAI®
Pour des systèmes d'information
de confiance et créateurs de valeur

Cloud computing et protection des données