e-@roit
ETUDE ROSENTHAL

CLOUD COMPUTING : ENJEUX «JURIDICO-ORGANISATIONNELS» ET CONTRACTUELS

INSOMNI'HACK

21 Mars 2014

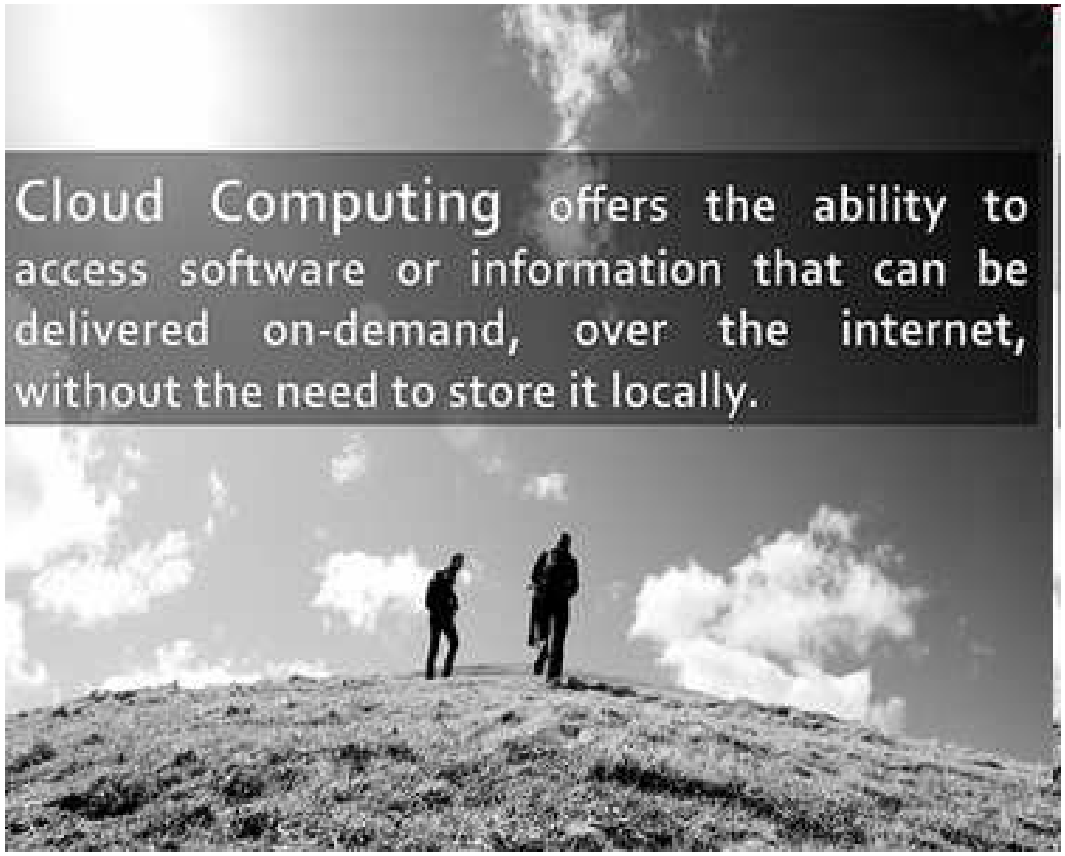
Nicolas Rosenthal

ORDRE DU JOUR

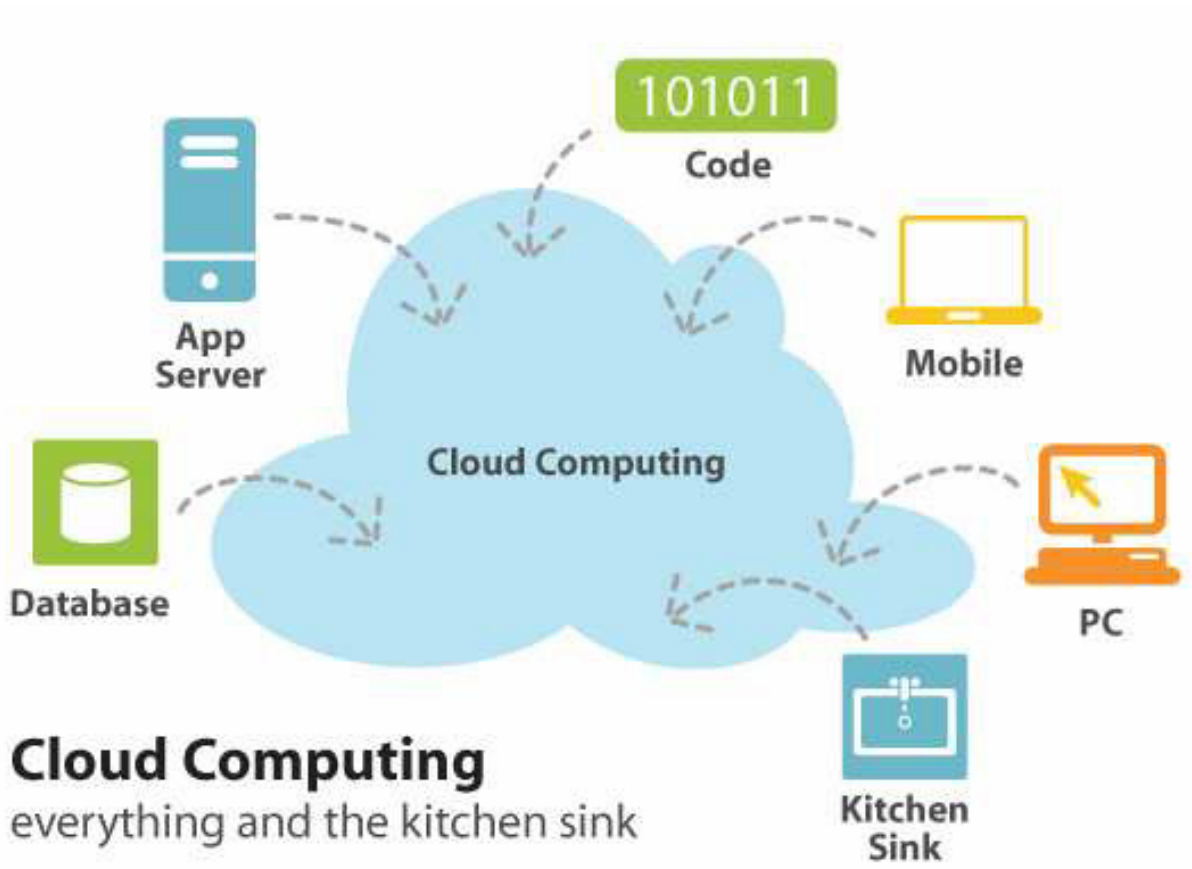
- Introduction: qu'est-ce que le cloud computing ?
- Sécurité des données dans le cloud !?
- Le rapport contractuel
- Questions et discussion

QU'EST-CE QUE LE 'CLOUD COMPUTING' ?

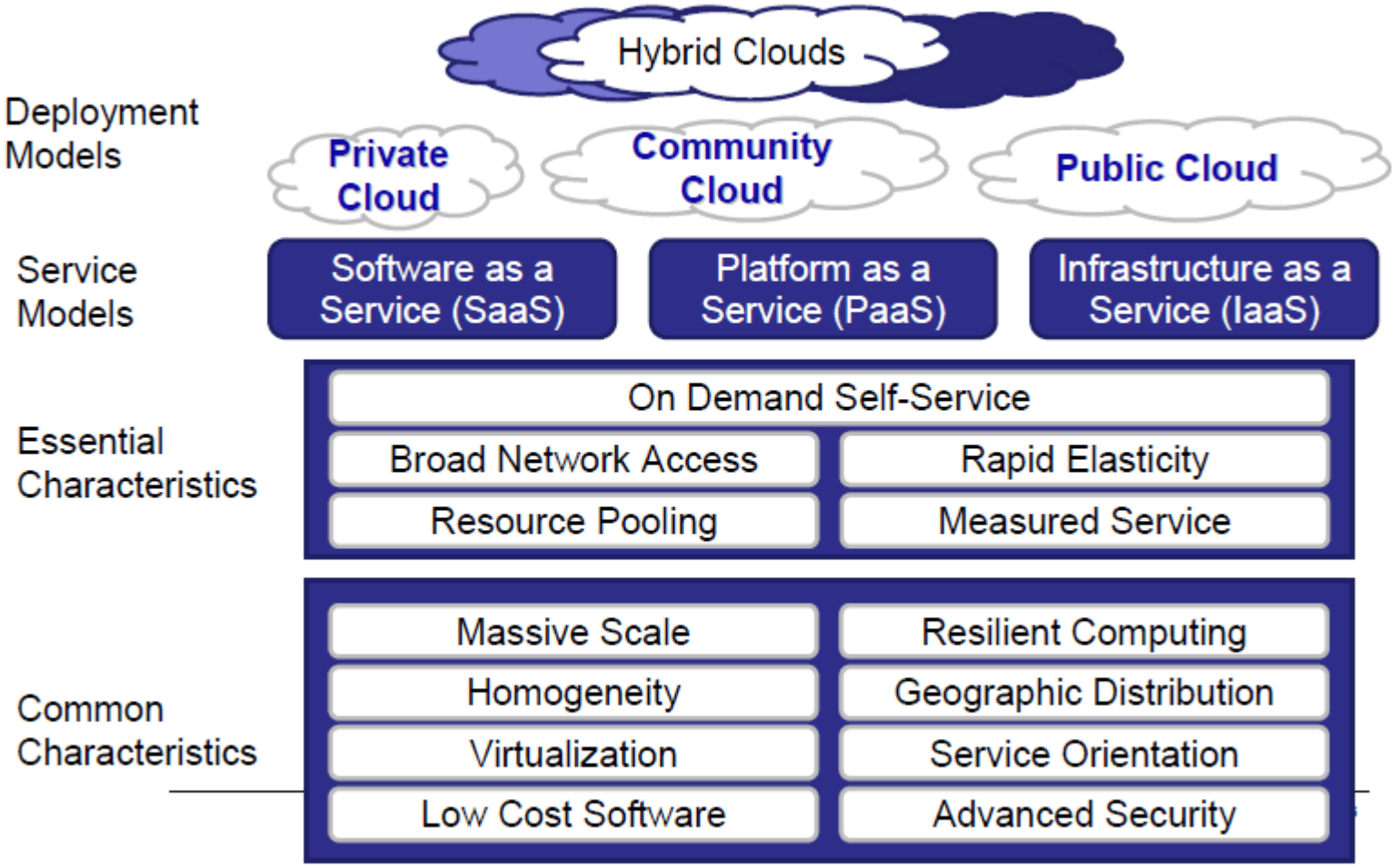
- Programmation dans le nuage
- Nombreuses définitions
- Effet de mode (?)
- Avancée technologique



RIEN D'AUTRE QU'UN FOURRE-TOUT ?

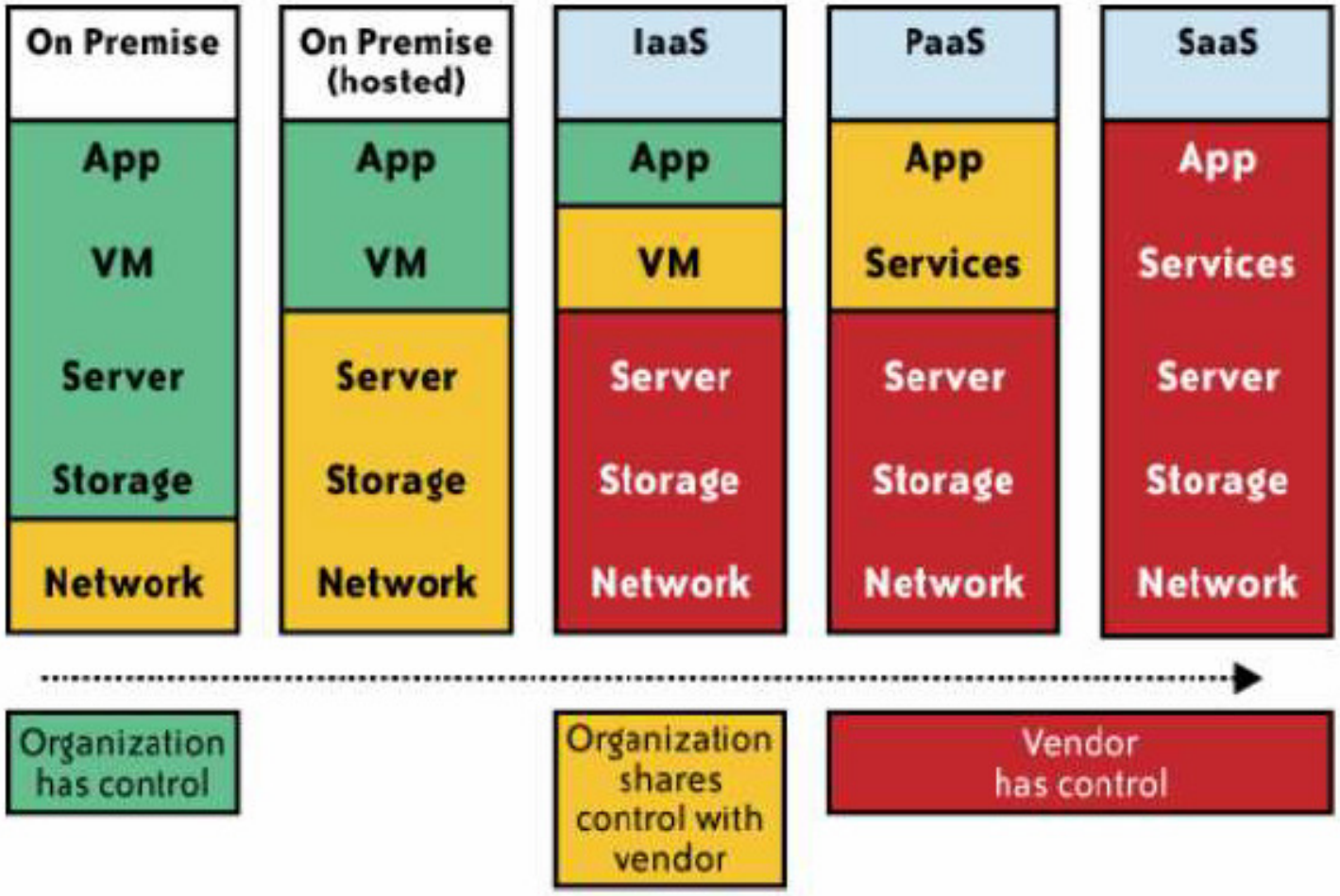


CADRE DE DEFINITION DU NIST

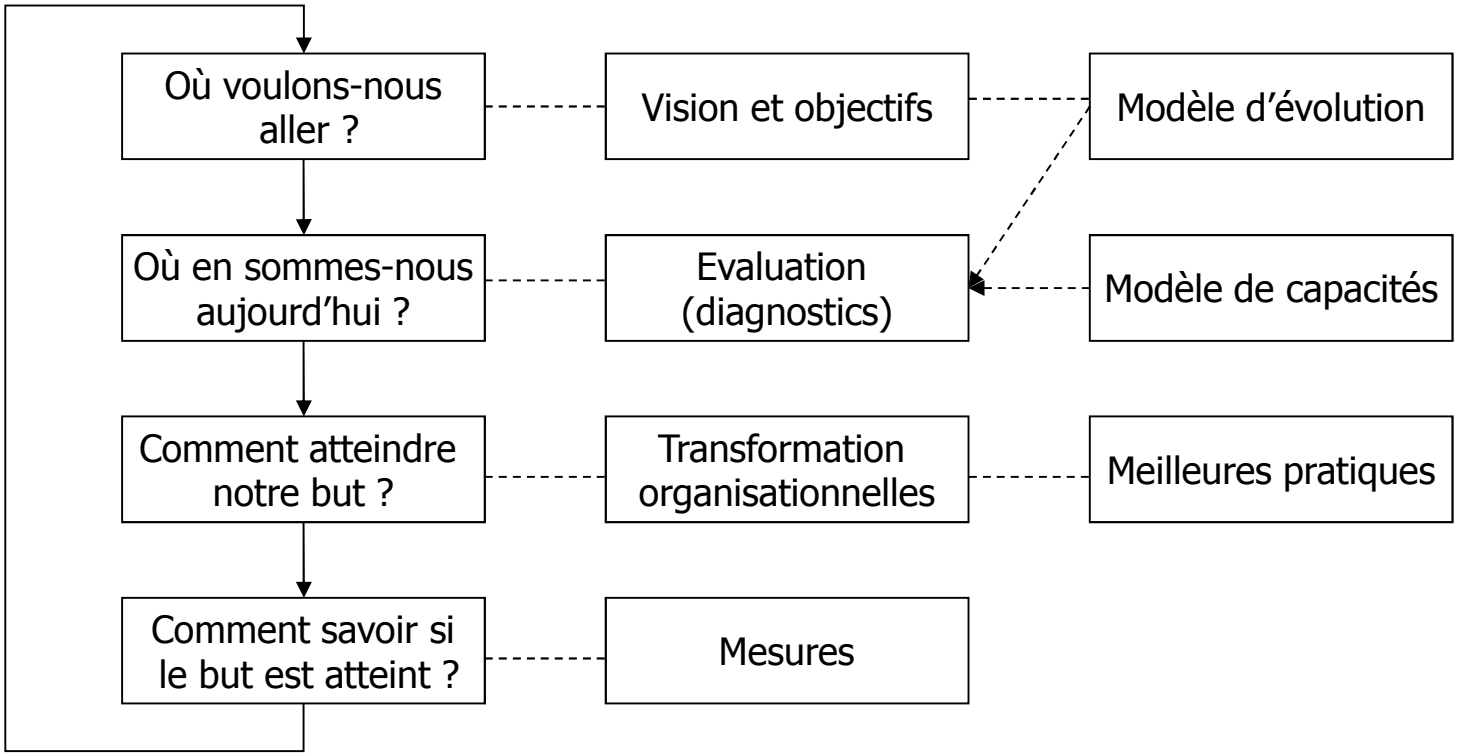


Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

QUI A LE CONTRÔLE SUR VOS RESSOURCES



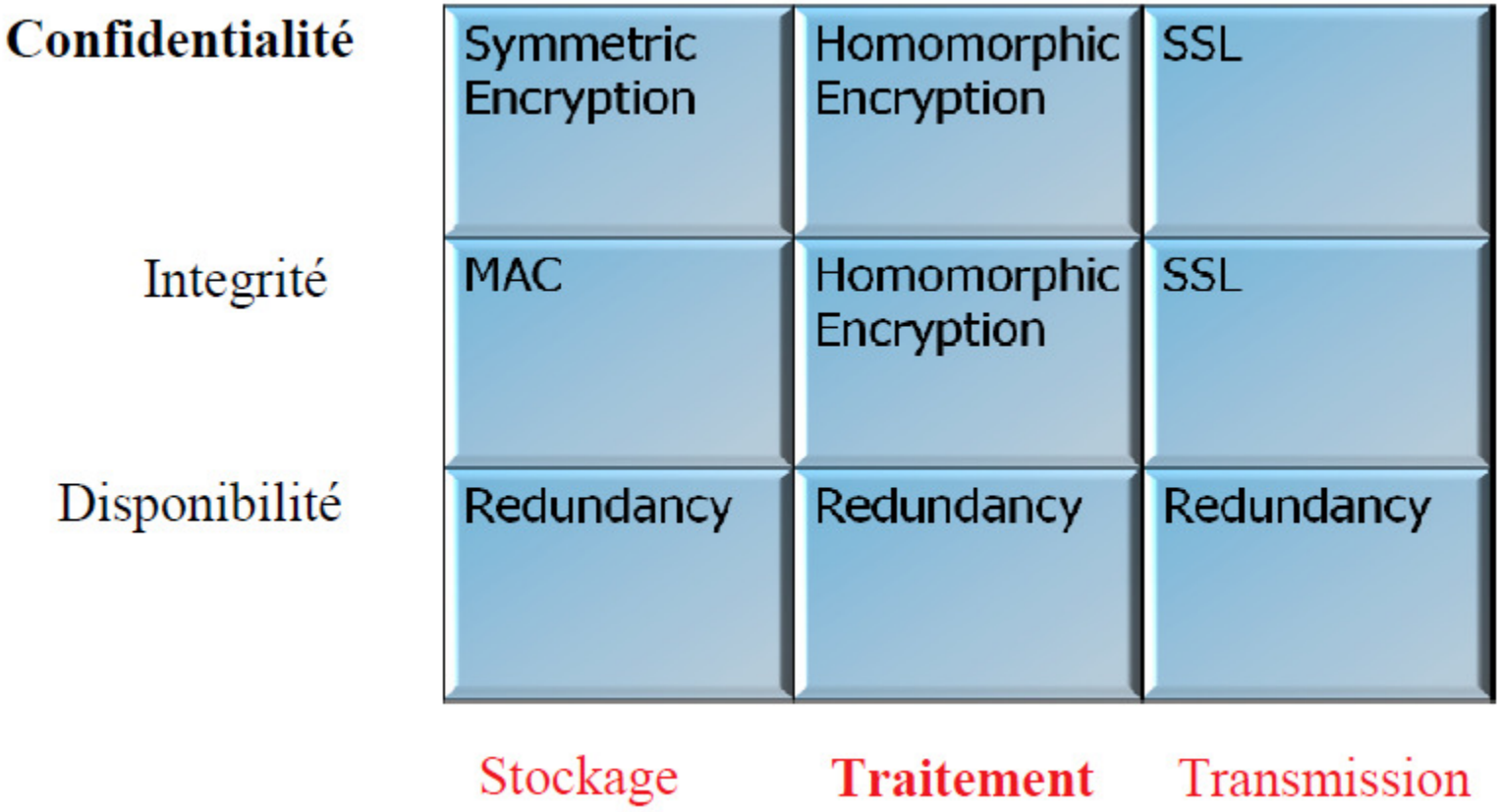
L'EXTERNALISATION : UNE STRATEGIE



RECOMMANDATIONS DE SÉCURITÉ DU BSI POUR FOURNISSEURS DE CLOUD COMPUTING

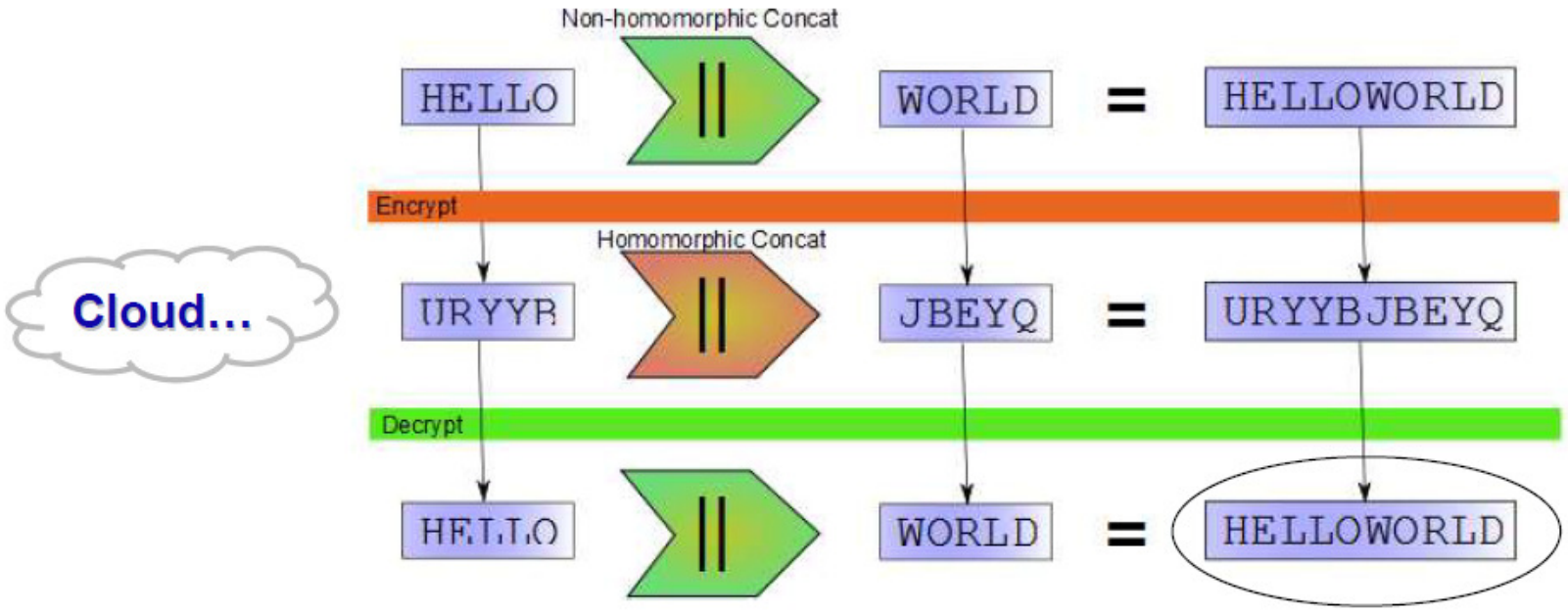
1. Gestion de la sécurité chez les fournisseurs de services Cloud
2. Architecture de sécurité
3. **Gestion des identités et des droits**
4. Possibilités de contrôle pour l'utilisateur
5. Gestion de la surveillance et des incidents de sécurité
6. Gestion des cas/situations d'urgence
7. Portabilité et interopérabilité
8. **Examen et preuve(s) de sécurité**
9. **Exigences envers le personnel**
10. Aménagement des contrats (transparence; SLA)
11. **Protection des données et conformité**

SECURITE DES DONNEES DANS LE CLOUD COMPUTING



CHIFFREMENT HOMOMORPHE

- "Homomorphe" est un adjectif qui décrit une propriété d'un schéma de chiffrement, c-à-d. la capacité d'effectuer des calculs sur le contenu chiffré sans devoir le déchiffrer!

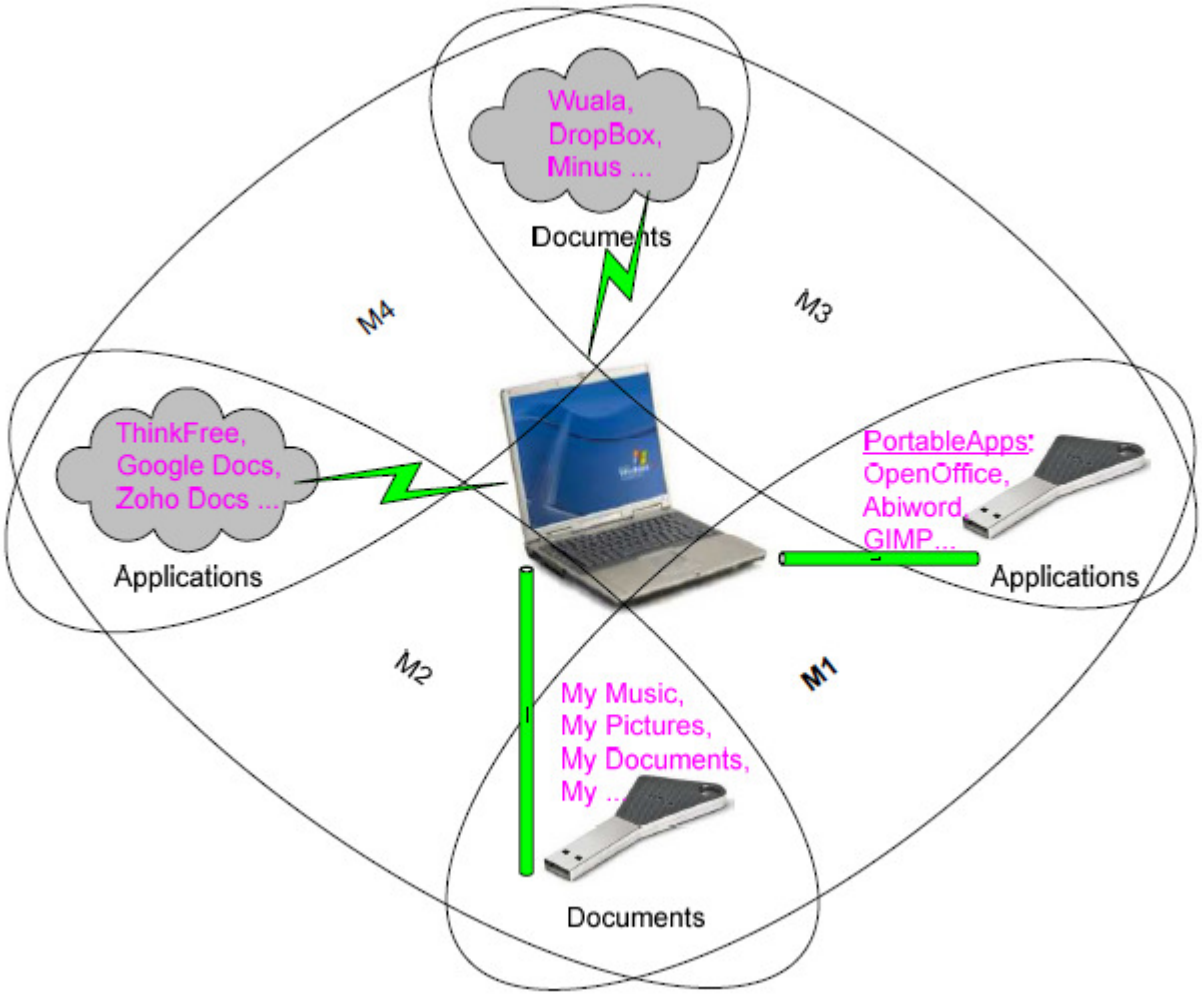


LE MONDE CLOUD IDÉAL VU PAR UN MATHÉMATICIEN

$$f(X_1, X_2, \dots, X_v) = \sum a_{e_1, \dots, e_v} X_2^{e_2} \dots X_v^{e_v} \bmod p.$$

$$Dec(sk, Eval(pk, (\alpha_1, \dots, \alpha_v), f)) = f(m_1, \dots, m_n)$$

CLOUD COMPUTING : PORTABLE SPACE ?



WILL THERE BE PRIVACY IN THE CLOUD?

Ted Rogers School of Information Technology Management Ryerson University - February 24, 2011 «Will There Be Privacy in the Cloud? … only if it's Embedded – by Design: Implications for the Future of Privacy»

Ann Cavoukian, Ph.D.Information and Privacy Commissioner Ontario

Privacy by Design : Les sept principes fondamentaux

1. **Proactif et préventif**, plutôt que réactif ou correctif…
2. Protection implicite de vie privée
3. Protection **intégrée** dans la conception (systèmes/pratiques)
4. Fonctionnalité **intégrale** : somme positive (non nulle !)
5. Sécurité de bout en bout : protection **durant tout le cycle de vie**
6. Visibilité et **transparence**
7. Respect de la **vie privée des utilisateurs** (au centre !)

- **www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf**

CONCEPTS ET DEFINITIONS DU CLOUD COMPUTING

- *A retenir :*

  - Le cloud computing désigne une informatique externalisée vers des lieux de traitement des données inconnus de ses utilisateurs. Il englobe les concepts de SaaS et PaaS.
  - On définit le SaaS comme le successeur de l'ASP, en y intégrant les bonnes pratiques issues du web : interface RIA, architecture multi-tenant, API ouvertes, orientation collaboration.
  - Les PaaS sont des plates-formes en ligne exploitables pour héberger des SaaS développés par des fournisseurs de services ou par les entreprises clientes elles-mêmes.
  - Le IaaS, c'est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur.
    - l'entreprise gère : les systèmes d'exploitation des serveurs, et surtout les logiciels applicatifs (exécutables, paramétrages, l'intégration SOA, les bases de données)
    - le fournisseur Cloud gère : le matériel serveur, les couches de virtualisation, le stockage, les réseaux.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La confidentialité des données**

- Le monde de l'entreprise est universellement et intimement persuadé que l'on doit conserver ses données informatiques dans ses locaux pour assurer leur sécurité.
- Cette intime conviction est un peu étrange quand on sait que les entreprises utilisent depuis des années les services de prestataires d'hébergement pour leurs applications web et leurs extranets clients ; des données parfois critiques concernant l'entreprise et ses clients transitent par ces tiers. La confiance accordée aux prestataires d'hébergement tient à leur réputation sur le marché, et à leurs engagements contractuels. En effet, ils s'engagent juridiquement au travers de « règles de confidentialité » à ne pas divulguer les données de leurs clients. Les opérateurs SaaS prennent les mêmes engagements, mais attirent moins la confiance que les prestataires d'hébergement. Selon nous, cette méfiance est essentiellement due aux origines des SaaS : ces acteurs sont issus du monde du web, un monde connoté grand public ; tandis que les prestataires d'hébergement sont issus du monde des télécoms, un monde connoté entreprise.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La confidentialité des données :**

- On peut considérer plusieurs typologies de risques :

  - **Risque de vol de secret industriel.** Ce risque existe dans les secteurs très concurrentiels, par exemple, ceux où le dépôt de brevet est critique pour s'assurer de nouveaux marchés.
  - **Risque de vol de données confidentielles sur ses clients.** Ce risque existe dans des secteurs comme celui de la banque, où la protection des données est critique.
  - **Risque de vol de données de fonctionnement interne.** Ce risque porte essentiellement sur l'image d'une entreprise connue. Si le public apprenait qu'on lui a volé des données, son image serait ternie.
  - ….

EXTRA-TERRITORIAL JURISDICTION
THE NOTORIOUS "SECTION 702" FISA AMENDMENTS ACT (FAA)

- xKeyscore: All VPN connections in Switzerland
- Threshold: from 'primary' to 'a' purpose
- Sealed Case, 310 F.3d 717: re-use in criminal proceedings
- 5 year extension on 31 Dec. 2012
- No legal safeguards for non-US persons

The United States [...] takes the position that it can use its own legal mechanisms to request data ***from any Cloud server located anywhere around the world*** *so long as the Cloud service provider is subject U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise* ***conducts continuous and systematic business in the United States.***

Even Acknowledged in U.S. Lobby paper:
Hogan Lovells 2012, p. 5.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La confidentialité des données :**

- Les entreprises gèrent ces risques au travers d'une «politique de sécurité» mise en œuvre par le « CIO »
- Parmi les documents issus de la politique de sécurité, on doit trouver une **classification des données** qui établit le degré de confidentialité des données manipulées dans l'entreprise. Cette classification permet de mener des « **analyses de risques** » sur les données lorsqu'on envisage leur externalisation, par exemple chez un opérateur SaaS. Ces analyses de risque intégreront bien entendu les possibilités d'écoutes sur Internet.
- La « classification des données » et l'« analyse de risques » sont des outils d'aide à la décision indispensables à tout arbitrage sur la sécurité des données.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

Quelles lois ?

- Quels pays ?
- Nouveau Règlement communautaire sur la protection des données
- LPD – OLPD
- CO (contrat de travail, contrat d'entreprise, contrat de bail…)
- CP (vol de données, soustraction de données, intrusion dans un système dument protégé…)
- Olico, LTVA…
- Les chimères : ex. fiscalité > délocalisation > « fraude » > blanchiment d'argent?
- Lois sectorielles : Circ. FINMA 2008-07…
- Lois cantonales…
- La normalisation ?
- La certification ISO….

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

La suprématie du droit suisse ?

- **Affaire GoogleStreetView**

  Dans son arrêt (ATF 138 II 346), le Tribunal fédéral s'est tout d'abord prononcé sur la compétence des autorités et tribunaux suisses quant à l'appréciation de l'état de fait. Un traitement de données est soumis au droit suisse de la protection des données et relève de notre compétence dès lors qu'un lien suffisant avec la Suisse existe - ce qui **est également le cas lorsque les serveurs sont stationnés à l'étranger**. Dans l'affaire Google Street View, des informations sur des personnes, des rues et des places en Suisse sont rassemblées et publiées, donc consultables sur internet depuis la Suisse. Cet arrêt est important en ce sens qu'il précise que la loi suisse sur la protection des données est également applicable à un traitement qui a lieu en partie à l'étranger lorsqu'un lien suffisant avec la Suisse existe.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La conformité règlementaire**

- Dans certains secteurs d'activité, les entreprises doivent respecter des contraintes légales très fortes. Par exemple, les lois Sarbanes-Oxley forment un cadre réglementaire strict. Le respect de contraintes légales peut être un frein très fort à l'adoption du modèle SaaS.
- Par ailleurs, les entreprises sont méfiantes vis-à-vis des applications SaaS hébergées dans d'autres pays ou sur d'autres continents, où les réglementations peuvent être différentes. Par exemple, un *datacenter* hébergé en Chine subit la réglementation chinoise, pays dans lequel l'autorité centrale peut demander à consulter les données stockées sur les serveurs. Les opérateurs SaaS proposent depuis peu à leurs clients de s'engager à ce que leurs données soient hébergées dans leur région, l'Europe, **voir la Suisse** par exemple. Ceci afin de leur garantir que leurs données ne tomberont pas sous le coup d'une réglementation tierce.
- La Loi Fédérale sur la Protection des Données peut imposer un formalisme auprès des clients et des collaborateurs (devoir d'annonce Circ. FINMA 2008-07) ainsi que de déclarer l'externalisation du traitement de données.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **LPD : tiers**

- En tant qu'entreprise, vous pouvez confier le traitement de données personnelles à un tiers dans la mesure où aucune obligation légale ou contractuelle ne vous impose de garder le secret. Mais en votre qualité de mandant vous devez veiller à ce que les données soient traitées de la même façon que vous seriez autorisé vous-même à le faire.
- **Le traitement de données ne peut être confié à un tiers que si la sécurité des données est assurée.**
- Le maître du fichier répondra du préjudice causé par le fait qu'il a confié le traitement à un tiers sans s'assurer de la sécurité des données.

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **LPD : tiers**

- Un système équivalent de protection des données ne garantit cependant pas à lui seul que toute atteinte à la personnalité pourra être évitée.
- **Il est donc conseillé dans tous les cas de rédiger des clauses spécifiques dans le contrat** avec le destinataire des données, contrat qui réglera la protection et la sécurité des données.
- Lorsqu'un fichier est transféré vers un Etat qui ne possède pas de système de protection des données équivalent, **il est obligatoire de conclure un tel contrat**.

- (NB : liste Safe Harbor) **http://www.export.gov/safeharbor**

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La réversibilité des applications et effacement des données**

- *On appelle réversibilité la capacité à quitter une solution informatique pour une autre. Cette réversibilité implique que l'on puisse récupérer ses données et éventuellement ses composants métiers chez son prestataire d'hébergement pour les migrer chez un autre acteur ou éventuellement les rapatrier en interne.*
- Les SaaS fournissent de nombreux assistants d'import pour permettre la migration des données vers leurs plates-formes. **Par contre, elles ne fournissent pas d'outils complets pour récupérer ses données. (pas d'ordonnancement de données)**
- Prenons l'exemple de Flickr, un service de stockage et de partage de photos ; cet opérateur SaaS dispose d'une offre premium payante destinée aux professionnels. Il fournit gratuitement un logiciel d'envoi de photos vers sa plate-forme : le « Flickr upload », mais il ne fournit pas de logiciel de « Flickr download » pour les récupérer en masse. Il est donc nécessaire de les récupérer une à une, ce qui est très fastidieux.
- Heureusement, on a vu que les SaaS fournissent des API permettant de se connecter à leurs plates-formes. Il est donc possible pour la DSI de développer des composants sur la base de ces API pour permettre la réversibilité. Ces composants sont souvent fournis par des éditeurs tiers (c'est le cas de du Flickr downloader).
- Quid de l'effacement des données chez l'opérateur (archivage, contraintes de conservation…)

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La dépendance au réseau de télécommunication et l'augmentation du trafic**

- La problématique de dépendance des SaaS au réseau est très réelle. Il convient cependant de la relativiser. En effet, sans le modèle SaaS, une rupture de réseau est déjà très critique pour de nombreuses entreprises. Elle implique :
  - Une rupture dans l'envoi et la réception de messages avec les clients ou partenaires.
  - Une rupture des flux de données avec les partenaires.
  - Une rupture de l'accès au site web ou/et à l'extranet pour les clients.
  - La perte de l'accès au web pour les collaborateurs.
- Il est donc indispensable pour les entreprises d'aujourd'hui de se doter d'un lien réseau de haute qualité avec la redondance adéquate pour pallier à des pannes.
- **L'argument de la dépendance au réseau avec les SaaS est donc un faux argument : aujourd'hui quasiment aucune entreprise ne peut travailler sans accès à Internet, avec ou sans SaaS !!!**

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **La dépendance au réseau de télécommunication et l'augmentation du trafic**

- Un autre argument souvent avancé par les informaticiens pour contester le modèle SaaS est l'augmentation du trafic réseau. En effet, des échanges qui avaient lieu sur le réseau interne de l'entreprise vont passer par le lien Internet avec le modèle SaaS.
- Par exemple, pour envoyer un message à un collègue via Google Apps, on le fait transiter deux fois par Internet : une fois pour le transmettre à la plate-forme Google, et une fois pour le collecter à partir de la plate-forme Google.
- *La problématique d'augmentation du trafic réseau est à considérer. Il convient néanmoins de la modérer. En effet, les SaaS proposent des interfaces web et les pages web ont un poids très modeste.*

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **Étudier les problématiques d'intégration**

- L'intégration de flux d'informations entre l'opérateur SaaS et l'entreprise peut revêtir différents niveaux de complexité :
  - 1/ Dans un scénario simple et fréquent, il se limite à la création manuelle de comptes utilisateurs chez l'opérateur.
  - 2/ Dans un scénario un peu moins simple, on peut souhaiter maintenir une **synchronisation** entre l'annuaire d'entreprise et la base de comptes hébergés chez l'opérateur.
  - 3/ Dans un scénario nettement plus complexe, on peut être amené à **échanger des flux d'informations en continu avec l'opérateur** SaaS.
- Le troisième type de scénario (3) est peu fréquent dans un contexte où le SaaS est utilisé pour de l'informatique de commodité. Il est cependant indispensable de bien anticiper ces contretemps car ils peuvent se révéler très lourds à gérer par la suite.
- Une étude de premier niveau des problématiques d'intégration est donc un préalable au choix d'aller vers une solution SaaS**.**

LES ENJEUX JURIDIQUES ET OPERATIONNELS DU CLOUD COMPUTING

- **Étudier la pérennité de l'opérateur SaaS-PaaS-IaaS**

- En parallèle de l'analyse de risque, il convient d'évaluer la pérennité de l'opérateur XaaS. En effet, la démarche de migration vers une plate-forme SaaS est une démarche lourde, dont la réversibilité est non triviale. Il est donc indispensable de s'assurer de la stabilité de son partenaire.

- Vérifier l'actionnariat voir monitorer l'actionnariat…

LES ENJEUX CONTRACTUELS

- La variété de la terminologie…

  Contrat d'externalisation
  Contrat d'outsourcing
  Contrat d'infogérance
  Contrat de facilities management (FM)
  Contrat de prestations informatiques
  Contrat de Cloud services….

Dans certain cas avant tout un contrat d'ADHESION…

LA PHASE DE CONTRACTUALISATION D'UN SaaS

Clarification

- **Le contrat d'infogérance** se définit comme un ensemble d'activités de services consistant en la prise en charge de la gestion de tout ou partie du système d'information d'une entreprise avec ou sans délocalisation.

- Il s'agit d'**un contrat d'entreprise Art. 363 CO**.

  Contrat par lequel une personne se charge de faire un ouvrage pour autrui, moyennant une rémunération, en conservant son indépendance dans l'exécution du travail.

  Les prestataires de tels services peuvent être des personnes indépendantes, des SSII mais également des constructeurs qui fournissent des offres de services connexes.

LA PHASE DE CONTRACTUALISATION

Obligation des parties : l' obligation de moyens et obligation de résultat

- **l'obligation de moyens** astreint le débiteur de l'obligation à employer les meilleurs moyens possibles en vue d'atteindre un résultat aléatoire (développer un logiciel, par exemple) ;
- **l'obligation de résultat** impose au débiteur l'obligation d'atteindre un résultat déterminé (développer un logiciel dont les spécifications prévoient un temps de réponse aux questions inférieur à deux secondes, par exemple).

La nature de ces obligations, moyens ou résultat, entraînera une différence notable en cas d'inexécution, quant à la charge de la preuve :

- dans le cadre d'une obligation de moyens, la charge de la preuve appartiendra au client : prouver que l'autre partie n'a pas exécuté ses obligations contractuelles ;
- dans le cadre d'une obligation de résultat, la charge de la preuve appartiendra au prestataire qui devra prouver qu'il n'a pu dûment réaliser sa prestation, et que cette défaillance ne lui est pas imputable.

LA PHASE DE CONTRACTUALISATION
La fin du contrat et sa résiliation

- **Les conséquences de la résiliation**
- Dans tous les cas de résiliation du contrat, les parties veilleront à envisager les conséquences de la résiliation, particulièrement importantes dans le domaine de l'informatique.
- Il pourra être envisagé, notamment :
  - la restitution des documents, des données et des programmes ;
  - l'engagement de ne pas conserver de copie par l'une des parties ;
  - l'accord éventuel sur le maintien de la confidentialité pendant une durée complémentaire ;
  - une période de réversibilité ;
  - le règlement des montants financiers qui resteraient dus, etc.
  - Les conséquences de la résiliation pourront varier selon les causes de résiliation.

CONCLUSION

- Parmi les catalyseurs clés à retenir poussant les organisations à considérer le cloud computing figurent : la recherche d'agilité et d'optimisation des coûts, la volonté d'accélérer les développements et déploiements, les possibilités offertes grâce à l'accès distant, l'intérêt de ne pas investir en matériels et logiciels (OPEX vs CAPEX) ;
- Néanmoins, des enjeux restent encore à relever : contrats complexes, confidentialité des données, intégration au système d'information, garantie de qualité et de continuité de service, dépendance au prestataire, problématiques réseaux… ;
- L'adhésion invisible au Cloud…
- Rester en Suisse, **encore possible ?!?**

APPROFONDIR SES COMPETENCES EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES www.appd.ch

- L'APPD, association de droit suisse, a notamment pour objet de promouvoir la Loi sur la protection des données, ainsi que le statut des Conseillers à la protection des données, des Maîtres de fichiers mais également de tout professionnel concerné par la gestion des données personnelles.
- Elle favorise la concertation entre les entreprises, les administrations et le Préposé fédéral à la protection des données et à la transparence.
- Elle maintient des relations avec le Préposé fédéral à la protection des données et à la transparence et avec toute autre instance cantonale ou européenne qui contribue à la protection des données personnelles.
- Elle formule des avis et des recommandations au Préposé fédéral à la protection des données et à la transparence, aux Préposés cantonaux à la protection des données, au Contrôleur européen à la protection des données, ainsi qu'aux acteurs de la protection des données personnelles.
- Elle développe, au travers de formations continues et des échanges entre ses membres, les meilleures pratiques professionnelles.
- Elle coopère avec les associations étrangères de même nature afin de garantir une harmonisation cohérente de la protection des données.

Je vous remercie de votre attention

Nicolas Rosenthal
m : +41 (0)76 332 11 11
t : +41 (0)21 711 26 06
rosenthal@e-droit.ch
www.e-droit.ch

Nicolas Rosenthal est un expert juridique indépendant qui dispose d'une vaste expérience tant de Conformité de systèmes d'information, de la Gouvernance d'entreprise, que du droit bancaire suisse et international. Il est le conseil juridique de nombreuses banques suisses et étrangères ainsi que de Fondations de droit suisse.

Il est reconnu comme une référence au sujet de l'autorégulation bancaire et des lois sur la protection de la sphère privée. Il est consulté par les autorités de régulation bancaire dans de nombreux pays. Il intervient auprès de Comités européens et internationaux sur les aspects juridiques et normatifs de la protection des données personnelles. C'est également le fondateur de l'Association des Professionnels de la Protection des Données www.appd.ch

Nicolas Rosenthal
Legal Adviser - Lead Auditor
Swiss citizen, born in Geneva (1973)

LL.M, PhD Lausanne University Law School, Switzerland
Laureate, Geneva WIPO Worldwide Academy, Switzerland
Master in Business Law, Montpellier University Law School, France
Master in Latin American Law, Montpellier University Law School, France
Lead Auditor ISO 27001, Geneva, Switzerland