canton de vaud
LIBERTÉ ET PATRIE

Direction
des systèmes d'information

Avenue de Longemalle 1
1020 Renens

Consultation relative à la stratégie suisse Cloud Computing

Affaire traitée par : J.Azzouz, DSI, jamal.azzouz@vd.ch, 021 316 25 87

Réponse à la Confédération: 10.2.12, info@egovernment.ch

Copie pour information : Chef du département des infrastructures VD, membre du CoPil eGov CH
Office des affaires extérieures VD

<u>Document 1</u> : Stratégie Cloud Computing des autorités suisses

Thème / §	Remarques et propositions
3. Vision, pages 5-6	Globalement, la vision proposée souffre d'un décalage important entre la volonté fortement affichée pour une évolution vers le Cloud computing (« slogans ») et les exigences en matière de sécurité, dont la difficile prise en compte reste à définir. Le « tout Cloud » qui ressort des libellés courts de la vision (slogans) est trompeur, raison pour laquelle nous formulons quelques propositions d'ajustement et de simplification ci-dessous, afin que l'ambition affichée reste crédible. Si un qualificatif adéquat devait être formulé globalement pour la vision, ce pourrait être « *Recours maîtrisé au Cloud et à la mutualisation des services entre autorités et partenaires, afin d'optimiser les coûts, les risques et la qualité des prestations*. ». Dans cet esprit, nous proposons que le point 3.3 (cf. ci-dessous) de la vision figure en premier (3.1).
3.1 Les autorités utilisent les offres Cloud, page 5	Il conviendrait de mettre en évidence ce qui se cache derrière des déclarations telles que « *suffisamment sûrs* » et « *des moyens auxiliaires appropriés leur permettent d'utiliser les services Cloud de manière responsable* ». Un des principaux enjeux dans la décision de passer dans un modèle Cloud consiste à s'assurer de la sécurité du service fourni en termes de Confidentialité, Intégrité et Disponibilité. Une analyse de risque au cas par cas est nécessaire. Nous proposons de renommer cette vision par ex. en « ***Les autorités utilisent au cas par cas les offres Cloud pertinentes*** ».
3.2 Les autorités proposent des services Cloud,	Le rôle premier des administrations est de fournir des prestations au public, sans forcément viser le rôle de fournisseur de prestations TIC. Ce dernier rôle relève surtout de la responsabilité des acteurs économiques (fournisseurs). Demeure réservée la stratégie à définir plus globalement en matière de « Government Data » et de mise à disposition par les administrations de leurs données auprès d'acteurs « clients

Thème / §	Remarques et propositions
page 5	– fournisseurs » (cf. aussi Principe str. S4). Proposition de reformulation : « ***Les autorités <u>peuvent</u> proposer des services Cloud ciblés et liés à leur mission de service public »***.
3.3 Cloud gouvernemental pour un besoin de sécurité élevé, page 6	Le Cloud gouvernemental communautaire est la solution idéale d'un point de vue sécurité qui puisse permettre de répondre à la volonté de mutualisation exprimée par les autorités. Les négociations contractuelles sont nettement simplifiées dans le cadre d'une synergie commune orientée optimisation des coûts de fonctionnement de l'administration dans son ensemble. Le cloud gouvernemental ne peut pas (ne doit pas) être réservé uniquement aux besoins de sécurité élevée. La vaste majorité des données gérées par les administrations publiques nécessite une sécurisation (confidentialité, intégrité, disponibilité) de niveau moyen. Seules très peu de données ne nécessitent aucune sécurité, ou *a contrario* une sécurité élevée. Nous proposons la reformulation suivante, ainsi qu'un positionnement en 1er (3.1) : « ***Cloud gouvernemental pour une réponse optimale aux besoins de sécurité et de mutualisation ».***
4.1 Principes str. - G1 – **Marché**, page 6	La sécurité tout comme la mutualisation ou la maîtrise des coûts sont des exigences importantes. La vérification des engagements contractuels de sécurité des fournisseurs doit pouvoir être faite à tout moment. Ce qui, dans la réalité d'aujourd'hui est déjà quasiment impossible. La qualification des fournisseurs agréés peut prendre plusieurs voies (droit des soumissions – législations sur les marchés publics, accords de type PPP –partenariat public-privé, groupements d'intérêts, …). Ce principe n'est donc pas pertinent et peut être **supprimé**.
4.2 Principes str. – G2 – **Cloud first**, page 6	Pour les mêmes raisons que celles énoncées ci-dessus, le Cloud ne peut être qu'une option parmi d'autres, en fonction du respect des exigences en matière de sécurité, de risques, de coûts, de qualité, … Comme le libellé de ce principe peut suggérer une obligation quelle que soit l'opportunité de la solution Cloud, nous proposons de le renommer en « ***Cloud option ».***
4.3 Principes str. – G3 – **Responsabilité propre,** p. 6	Préciser que, afin d'assumer la responsabilité de l'utilisation du Cloud, l'utilisateur doit être rendu attentif aux risques et les accepter en toute connaissance de cause.

Thème / §	Remarques et propositions
4.4 Principes str. – G4 – **Souveraineté nationale**, page 6	Ce paragraphe n'est **pas assez restrictif**. En considérant les processus centraux critiques, la disponibilité évoquée dans le deuxième paragraphe est une préoccupation mineure d'un point de vue sécurité. Les risques sont bien plus importants en cas d'atteinte à l'intégrité ou à la confidentialité. L'intégrité des processus est tout aussi importante que l'intégrité des données. Le traitement et/ou l'hébergement des données en dehors du territoire Suisse constituent une prise de risque considérable, ceci d'autant plus que l'évolution de la scène politique, même à court terme, est imprévisible. Aujourd'hui déjà, des pays (USA, Chine, Russie, Israël, France, …) s'engagent officiellement dans la voie de la cyberguerre en constituant de véritables armées numériques. Il est donc difficilement argumentable d'un point de vue de la souveraineté nationale d'outsourcer une partie de l'informatique dans de tels pays. Par ailleurs et à titre d'exemple de difficulté à gérer en matière de souveraineté, une entreprise qui emploie des citoyens américains est indirectement soumise au Patriot Act, puisque les employés en question ont l'obligation de fournir aux autorités américaines les données qui leur seraient demandées.
4.5 Principes str. – G5 – **Gestion TIC globale**, page 7	Il faut mettre en place une structure de coordination légitimée et soutenue par toutes les parties prenantes.
4.6 Principes str. – G6 – **Fournisseurs de prestations TIC en tant qu'intégrateurs**, page 7	Dans ce cas, le fournisseur de prestations TIC assume toutes les responsabilités liées à la sous-traitance éventuelle, pour autant qu'elle ait été explicitement autorisée par le(s) mandant(s) et concrétisée dans les contrats, notamment en matière de souveraineté nationale et de dédommagement en cas de problème. Ces **restrictions** de la sous-traitance devraient donc être mentionnées.
4.7 Principes str. – G7 – **Normes**, page 7	Ce principe est **redondant** avec celui adopté dans le cadre de la stratégie nationale de cyberadministration (cf. art 4 de la **convention-cadre de collaboration** 2007-2015 [2]).
4.8 Principes str. – G8 – **Pas d'action isolée des**	

Thème / §	Remarques et propositions
autorités, page 7	
5.1 Principaux axes stratégiques - S1 – **Promotion de l'utilisation responsable du Cloud**, p. 7	Pour demander aux autorités une utilisation responsable du Cloud, il conviendrait préalablement d'évaluer la confiance qu'elles peuvent accorder aux fournisseurs : la labellisation et un processus de certification régulier sont donc nécessaires pour assurer une promotion efficace du Cloud.
5.2 Principaux axes stratégiques - S2 – **Adaptation des bases légales**, page 8	La prise de position est bien **trop catégorique**. On ne peut décemment prôner l'abrogation de toutes les lois existantes sous prétexte qu'elles freinent le déploiement d'une nouvelle architecture des services IT. Les lois peuvent être réexaminées pour statuer sur leur assouplissement potentiel afin de permettre la rationalisation du système d'information et la modernisation de l'Etat, notamment via le recours à des solutions mutualisées et/ou utilisant le Cloud à certaines conditions. Par ailleurs, ce principe est **redondant** avec celui adopté dans le cadre de la stratégie nationale de cyberadministration (cf. art 3 de la **convention-cadre de collaboration** 2007-2015 [2]).
5.3 Principaux axes stratégiques - S3 – **Mise en place d'offres Cloud dédiées pour les autorités**, page 9	Le Cloud communautaire ne devrait pas être cantonné à une affectation haute sécurité mais supporter plus largement la mutualisation des ressources et des services à travers les cantons, les communes et la Confédération.
5.4 Principaux axes stratégiques - S4 – **Mise en place d'offres Cloud pour les privés et l'économie**, page 10	Comme déjà mentionné ci-dessus (3.2, …), ce n'est pas le rôle de l'Etat de proposer un Cloud pour les privés et l'économie. Le « mélange des rôles » créerait un vrai casse-tête sécuritaire. **A supprimer.**

Thème / §	Remarques et propositions
5.5 Principaux axes stratégiques - S5 – **Collaboration avec l'économie et l'environnement international**, page 10	Autre thème mais même remarque, ce n'est pas le rôle des autorités de porter ce genre d'initiative. **A supprimer**.
6 Mise en œuvre, page 11	Le Cloud gouvernemental est le projet le plus intéressant d'un point de vue sécurité et opportunité (maîtrise des coûts et des risques) ; il devrait être privilégié selon les 3 axes : IaaS, PaaS et SaaS. Le Cloud computing pour les administrations publiques doit être exclusivement consacré à la fourniture de prestations pour l'exécution des tâches supportant le service public. Cf. remarques ci-dessous sur le catalogue de mesures de mise en œuvre de la stratégie Cloud computing.

Direction des systèmes d'information – DSI
Avenue de Longemalle 1, CH 1020 Renens
www.vd.ch – Tél: +41 21 316 26 00 – Fax: +41 21 316 27 26

Document 2 : Catalogue de mesures soutenant la stratégie Cloud Computing des autorités suisses

Thème / §	Remarques et propositions
1. Introduction - page 3	La vision et les objectifs stratégiques en découlant sont très (trop) ambitieux. Une priorisation des objectifs et projets de mise en œuvre est nécessaire, dans le cadre de la feuille de route eGov CH (CoPil) : - traitement des pré-requis avant les prestations - sélection des mesures de ce *catalogue Cloud* en fonction de leur contribution concrète et directe aux pré-requis et prestations prioritaires du *catalogue eGov CH* [1], tels que reformulés dans le nouveau *plan d'action 2012-2015* découlant de la *convention-cadre* [2] de collaboration entre Confédération, cantons et communes - prise en considération des besoins des cantons, des communes et de la Confédération

[1] http://www.egovernment.ch/dokumente/katalog/E-Gov-CH_Katalog_2011-10-24_F.pdf

[2] http://www.egovernment.ch/dokumente/rv/2007-2015/E-Gov-CH_Rahmenvereinbarung-2007-2015_F.pdf