# Le référentiel de l'ANSSI se fait attendre

Mais que diable fait l'ANSSI avec le document que tous les acteurs français du Cloud attendent avec impatience : Le référentiel de qualification de prestataires de services sécurisés d'informatique en nuage.

Suite à la diffusion de la dernière version de travail (v1.3) le 20 juillet 2014, l'ANSSI avait lancé un appel à commentaires avec une date de clôture fixée au 3 novembre 2014. Cela fait donc bientôt un an que cette « dead line » est passée et depuis silence radio ! Combien de temps faudra-t-il encore à l'ANSSI pour prendre en compte les différentes remarques et les autres initiatives (Secure Cloud, Cloud confidence) et publier un référentiel définitif ?

Le référentiel de qualification de l'ANSSI contient des exigences et recommandations à destination des prestataires de services d'informatique en nuage. La qualification permet d'attester de la conformité du prestataire aux exigences du Référentiel. Pour cela, un organisme de qualification désigné par l'ANSSI est chargé de vérifier que le prestataire respecte les exigences (chapitres 5 à 18) par un audit du prestataire. Concernant les recommandations indiquées dans le référentiel, elles sont données à titre de bonnes pratiques et ne font l'objet d'aucune vérification en vue d'obtenir la qualification.

Le référentiel propose deux niveaux de qualification des prestations de *cloud* :

- le premier niveau, dit élémentaire, est conçu pour offrir un niveau de protection équivalent à celui requis par la PSSIE
- le second, dit standard, qui offre une protection plus robuste et permet notamment d'envisager le traitement de données sensibles de niveau Diffusion Restreinte.

Que peut-on dire de la version v1.3 diffusée par l'ANSSI le 20 juillet 2014 ?

Globalement, ce référentiel est assez décevant. On a l'impression qu'il a été rédigé en réalisant une adaptation de la norme ISO 27002 à la problématique de sécurité dans le Cloud. D'ailleurs, la structure du référentiel est un véritable copier/coller de la norme ISO 27002.

Pour ma part, j'ai formulé les remarques suivantes :

- Il n’y a aucune distinction effectuée entre les différents prestataires (IaaS, PaaS et SaaS) malgré les différences fondamentales en matière de sécurité et de responsabilités entre prestataires et clients,
- Il n’est fait aucune référence aux normes ISO internationales relatives au Cloud (ISO 17788, 17889, 27017, 27018). Même si ces normes sont très récentes, les drafts sont disponibles depuis très longtemps,
- Il n’y a aucune exigence concernant la disponibilité minimale des services,
- Il n’y a aucune exigence concernant la réversibilité des données (mesure totalement indispensable à la maitrise des données externalisées),
- Il y a par contre de très forte exigence nationale (localisation des données exclusivement sur le territoire français, support de premier niveau francophone localisé en France, contrat de droit français, tribunal compétent français, etc…) à tel point que l’on ne comprend pas comment l’ANSSI peut parler d’un référentiel ouvert doté d’une ambition européenne.

Les plus optimistes ont le droit de penser que l’ANSSI a bien pris en compte toutes les remarques formulées par les différents contributeurs et qu’un tout nouveau référentiel devrait sortir dans les prochains jours. Wait and see…