AWS : « surprenante » certification ISO 27017

Chad Woolf, Directeur risques et conformité chez AWS, a déclaré le 30/11/2015 sur le blog officiel d'Amazon : "*I am happy to announce that AWS has achieved ISO 27017 certification*".

Cette annonce est pour le moins surprenante car contrairement à l'ISO 27001, la norme ISO 27017 ne décrit pas un processus de gestion mais fournit un guide de bonnes pratiques. Elle a été développée par l'ISO pour compléter le guide initial définie par l'ISO 27002 et propose un ensemble de mesures de sécurité destinées à améliorer la sécurité des services dans le cloud.

En pratique, AWS a réactualisé son SMSI (pierre angulaire de l'ISO 27001) et mis à jour sa DdA (Déclaration d'Applicabilité) en adoptant les bonnes pratiques de l'ISO 27017. AWS a ensuite demandé à Ernst & Young de procéder à un nouvel audit pour attester de la prise en compte de l'ISO 27017 dans sa démarche ISO 27001.

On peut ainsi lire dans le certificat 27017 d'AWS : *" … certified under certification number [2013-009], is also compliant with the requirements as stated in the standard : ISO/IEC 27017:2015 "*
(*pour information, le numéro de certification [2013-009] correspond au certificate ISO 27001 d'AWS)*

En d'autres termes, Ernst & Young atteste que le SMSI d'AWS prend en compte les bonnes pratiques issues de l'ISO 27017 ce qui n'apporte en soi aucune information précise sur le niveau de sécurité effectif du fournisseur. En effet, en l'absence de publication de la DdA, on ne sait strictement rien sur la façon dont les mesures de sécurité proposées par l'ISO 27017 sont réellement implémentées au sein du SMSI d'AWS. Il s'agit donc encore une fois d'une démarche purement marketing, destinée à rassurer le client perdu dans la jungle des normes ISO/IEC 270xx. Dans le même état d'esprit, AWS aurait pu également demander à Ernst & Young un certificat ISO 27002 puisque naturellement son SMSI s'appuie sur des mesures issues de l'ISO 27002. Et pourquoi ne pas demander dans la foulée un certificat ISO 27005 puisque l'analyse de risque effectuée par AWS s'appuie sur ce référentiel ?