Commentaires sur le référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage

Le référentiel qu'a publié l'ANSSI concernant les exigences applicables aux prestataires de Cloud est une initiative utile qui participe à la promotion de la confiance dans l'informatique en nuage. Il appelle néanmoins quelques commentaires.

Ce cadre répond à la nécessité pour les pouvoirs publics de préciser leurs exigences pour le déploiement des services Cloud pour les entités publiques, dans le périmètre des fonctions régaliennes de l'Etat, en fonction des risques et de la nature des informations qu'elles traitent.

L'essor du Cloud est bénéfique aux organisations de toute taille et de tous les secteurs. Afin de le soutenir, il conviendrait de rationnaliser ce qui s'apparente aujourd'hui à une multiplicité de référentiels, dont l'existence fait peser des coûts importants pour les acteurs dans ce domaine, dans le cadre d'une concurrence internationale forte, alors même que l'Europe tente de créer un marché intégré du numérique.

Dans son champ de compétences, l'ANSSI peut être un acteur essentiel de cette rationalisation en soutenant la pertinence des normes internationales qui servent déjà de référence aux acteurs économiques du Cloud afin que l'ensemble des acteurs, et notamment les nouveaux entrants du marché, les adoptent, à coûts maitrisés.

La sécurité, la confidentialité et la conformité aux normes sont des responsabilités partagées entre les acteurs du Cloud et leurs clients du secteur privé. De même, lorsque leur client est l'Etat, ces acteurs ont à cœur de fournir le meilleur service en termes de disponibilité et de sécurité, tout en procédant à une optimisation des coûts d'opération, rendue nécessaire du fait des contraintes budgétaires.

1. Le périmètre d'application du référentiel

Au regard du champ de compétences de l'ANSSI et de sa capacité de contrôle, **notre compréhension est que ce référentiel a vocation à s'appliquer aux seules entités régaliennes de l'Etat** qui nécessitent un niveau de sécurité spécifique.

Les exigences du référentiel en matière de niveau de sécurité **ne sont pas adaptées aux besoins du marché en général et notamment à ceux du secteur privé**. Par contre, **le projet de Label Secure Cloud** proposé par le plan industriel Cloud, en cours d'élaboration, devrait pourvoir aux besoins du secteur privé en matière de bonnes pratiques, dans un contexte d'intégration d'un marché européen du Cloud. Il n'est donc pas opportun que ce référentiel devienne une référence de bonnes pratiques pour le secteur privé.

Par ailleurs, en l'état, les exigences imposées par le référentiel, s'ajoutant à certaines normes internationales, et ainsi que la référence explicite à la classification du niveau de sécurité des données telle que spécifiée par l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, désignent clairement le champ des entités régaliennes de l'Etat.

- Afin de ne pas entamer la compétitivité des acteurs du Cloud en France**, nous recommandons que ce référentiel se place délibérément et clairement hors champ du marché privé** afin qu'il ne puisse être affiché comme guide de bonnes pratiques pour ce marché, sauf à vouloir faire peser à ses acteurs des contraintes disproportionnées ou inadaptées aux besoins de leurs clients.

De plus, nous recommandons que **le champ d'application du référentiel n'intègre pas les Opérateurs d'importance vitale (OIV)**, étant donné que la plupart sont des acteurs privés. Si la Loi de Programmation Militaire a pour objectif le maintien en condition opérationnelle d'un certain nombre d'infrastructures critiques, elle ne dispose pas que tous les systèmes SI, même ceux des OIV, relèvent de ce cadre. En l'état de sa rédaction, le référentiel est potentiellement source d'insécurité juridique pour les OIV et leurs prestataires.

Sur ce point, il conviendrait que l'ANSSI clarifie dans quelle mesure l'utilisation du Cloud par le système d'information (interne) d'un OIV pourrait affecter la délivrance (externe) et la résilience de ses services à ses usagers ou à ses clients dans le cadre d'un service public opéré, par exemple, par délégation.

- A ce titre, **il serait utile de connaître quel est la perception du rôle que l'ANSSI attribue au Cloud et aux services Cloud dans le cadre de la résilience** du service ou de la continuité des missions de l'Etat.

- Le terme « **entité** » et le champ qu'il recouvre devrait ainsi être clarifié dans le référentiel, même si la liste complète des opérateurs d'importance vitale n'est connue que par les autorités administratives qui ont à la connaître.

2. Référencer clairement les normes internationales, dans leur intégralité

Le texte du référentiel comporte **un ensemble d'extraits de normes internationales**, telle que la norme ISO 27001, dont l'AFNOR est garante, mais sans y faire référence de manière explicite.

Au moment où la France et l'Allemagne ont décidé de porter une initiative européenne à même de conforter un espace de confiance numérique européen, le risque de la popularisation des exigences spécifiques d'un tel référentiel aux autres pays européens peut potentiellement **augmenter fortement les coûts pour tous les acteurs de l'informatique en nuage**.

S'il est légitime que l'Etat, via l'ANSSI, impose des exigences de haut niveau à même de répondre aux besoins spécifiques de ses missions régaliennes, il conviendrait d'exclure l'ambition de créer une norme « franco-française ».

En termes de définition de ce qu'est le Cloud et les services Cloud, **ce document devrait ainsi s'appuyer en matière de taxonomie sur la norme ISO/IEC 27000**, qui a été complétée de façon pertinente par la norme ISO/IEC 17788 « Technologies de l'information, Informatique en nuage ».

- Si l'Etat, à travers l'ANSSI, souhaite soumettre les acteurs du Cloud à des obligations supplémentaires pour ses objectifs spécifiques de sécurité de ses entités régaliennes**, il serait utile que l'agence clarifie la présentation de son référentiel** en faisant d'une part référence explicitement aux normes en vigueur et en listant séparément, d'autre part, ses exigences spécifiques et supplémentaires.

- Nous suggérons ainsi la prise en compte de la série des normes ISO/IEC « Technologies de l'information », « Techniques de sécurité », « Systèmes de management de la sécurité de l'information » dans la rédaction du référentiel, afin de clarifier les obligations des acteurs du marché, soit :

  - ISO 27000-2009 « Vue d'ensemble et vocabulaire »
  - ISO 27001-2013 « Exigences »
  - ISO 27002-2013 « Code de bonne pratique pour le management de la sécurité de l'information »
  - ISO 27005-2011 « Gestion des risques liés à la sécurité de l'information »
  - ISO 27009 Application sectorielle de la norme ISO/IEC 27001 – Exigences (en cours d'élaboration)
  - ISO 27034-1-2011 « Sécurité des applications » qui fournit un modèle pour intégrer la sécurité dans le cycle de vie des applications
  - ISO FDIS 27040 « Sécurité de stockage ».

En effet, **l'ANSSI doit pouvoir jouer un rôle dans l'harmonisation des référentiels nationaux**, afin d'accélérer l'usage d'une même base d'exigences de sécurité, simplifiant la compréhension de tous les acteurs économiques (et de leurs clients) de l'enjeu de la confiance dans le numérique, englobant à la fois sécurité, respect de la vie privée et protection des données.

Cela permettrait une mise en conformité des services d'informatique en nuage sur une base commune pour une pratique européenne permettant aux acteurs Français de hisser leurs offres au niveau des plus hauts standards.

- Dans ce but**, il serait nécessaire que le référentiel ANSSI se réfère aussi aux nouvelles normes, telle la norme ISO 27018**[1] (publiée en 2014), qui ajoute une somme de contrôles supplémentaires aux normes 27001 et 27002 **afin de pourvoir aux exigences de sécurité des données personnelles et de protection de la vie privée** (seule norme en l'espèce) ; le futur règlement européen sur les données personnelles intègrera des obligations que cette norme sait d'ores et déjà couvrir. De plus, cette norme éclaire le partage des responsabilités entre le client et le prestataire de service d'informatique en nuage en fonction des catégories de services comme le IaaS, PaaS ou SaaS.

- De même, il serait souhaitable que le référentiel **intègre la norme ISO 27017**[2] **en matière de sécurité du Cloud** (en cours de finalisation), sauf à apparaître rapidement caduque au regard des standards du marché.

- Enfin, nous recommandons que le référentiel **fasse référence à la norme ISO 19086** (en cours de finalisation) **qui explicite la notion de niveau de service (SLA)**, tout en faisant clairement la distinction entre les notions de fournisseur de Cloud, de responsable du traitement des données et de sous-traitant.

[1] ISO/IEC 27018-2014 Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

[2] ISO/IEC 27017 Code de bonne pratique pour le management de la sécurité de l'information fondé sur la norme ISO/IEC 27002 pour l'informatique en nuage, en cours de finalisation et attendue pour octobre 2015

3. Clarifier les différentes catégories de services cloud : IaaS, PaaS, SaaS

De manière générale, **le référentiel souffre d'un manque de distinction des différentes catégories de services (IaaS, PaaS, Saas)** ce qui entraine un manque de clarté concernant les différentes responsabilités des acteurs impliqués[3]. Au-delà, ce manque de précision pourrait être non conforme au regard de la réglementation nationale et européenne.

Ainsi, le document mentionne le rôle « de prestataire » sans distinguer la catégorie de service attachée à ce rôle, alors que les exigences ne s'appliquent pas de la même manière à tous les services. **Le rôle et les responsabilités afférentes au client/utilisateur mériteraient aussi d'être bien détaillés**, selon le contexte[4].

- A la fois dans ses exigences et recommandations, nous souhaitons souligner **la nécessité que le référentiel distingue les différentes catégories de services** ainsi que les différents rôles (client, prestataire, responsable du traitement, etc.) et les responsabilités afférentes qui leur incombent.

- La « transmissibilité » des exigences entre les différents rôles, des prestataires aux partenaires des différents services Cloud devrait aussi être détaillée.

- Afin que le référentiel soit conforme avec la règlementation concernant le partage des responsabilités dans le domaine de la protection des données personnelles, il devrait préciser les obligations des acteurs, responsable du traitement ou sous-traitant, dans leurs relations avec la Commission Informatique et Liberté[5].

- Enfin, il conviendrait **que le référentiel fasse référence à la norme ISO/IEC 17788 qui distingue d'autres catégories de services Cloud**, absentes du référentiel, telles le **DSaaS** (Data Storage as a Service) et le **CompaaS** (Compute as a Service).

[3] Par exemple, dans le cas de figure d'un service IaaS : comme le client peut chiffrer toutes ses données, le prestataire ne peut y accéder et en conséquence ne peut être tenu responsable de la conformité réglementaire. Autre exemple, celui d'un service SaaS : puisque le prestataire n'a pas connaissance des données traitées, la responsabilité du respect de la conformité réglementaire ne peut lui incomber.

[4] Dans le contexte du Cloud, le client/utilisateur a la responsabilité de choisir les données qui veut confier au prestataire. C'est à lui, et non au prestataire, de s'assurer si les données clients sont soumises à une classification particulière selon un référentiel extérieur.

[5] Cf section 6.3 « Relations avec les Autorités »

4. Niveaux de qualification des prestations Cloud et niveaux de sécurité

Le référentiel traite des modalités de qualification des prestataires de l'informatique en nuage, permettant d'attester leur conformité aux exigences décrites. Mais le référentiel manque de précision sur les modalités, notamment celles pour qu'une entité soit reconnue comme organisme de qualification habilité. Il serait souhaitable qu'il détaille la portée de la qualification.

- Il conviendrait que le référentiel décrive ou renvoie à une description du processus et du cahier des charges spécifiant les habilitations, leur durée et la liste des organismes habilités, afin d'éclairer les acteurs du Cloud.

- Il serait utile que le référentiel prenne en compte la complexité des services afin de mettre en regard la portée de la qualification, plus particulièrement pour les modèles SaaS et PaaS. En complément, il serait souhaitable qu'il apporte des précisions sur les cas de services construits sur la fondation d'autres services, qui ont des niveaux de qualification différents.

En ce qui concerne **les niveaux de sécurité**, **le référentiel apparaît inutilement restrictif, au regard de la réalité des besoins**.

En effet, les deux seuls niveaux de qualification des prestations désignés, dits « élémentaire » et « standard », en renvoyant à la seule catégorie de données « sensibles » restreint drastiquement le champ d'application des règles que souhaite imposer l'Etat. Ceci exclurait de nombreux besoins susceptibles d'être couverts par les services d'informatique en nuage, comme par exemple pour l'Open Data ou pour l'hébergement de messageries ne relevant pas d'un caractère « sensible » ou de « diffusion restreinte ». Par ailleurs, **le référentiel gagnerait en clarté s'il explicitait avec précision la notion de « données sensibles »**.

- Il serait hautement **souhaitable qu'au moins un niveau supplémentaire, avec moins d'exigences, ou « niveau élémentaire », soit ajouté** afin d'accueillir des données non sensibles. Un autre niveau intermédiaire pourrait également faire l'économie du chiffrement intégral de toutes les données.

- Par ailleurs, si le référentiel devait malgré tout s'appliquer à certains OIV, il conviendrait d'introduire un niveau supplémentaire et particulier équivalent au niveau « standard » décrit, mais permettant de traiter spécialement les données d'entreprises, en dehors de la sphère publique, qui sont concernées par le niveau dit de « Diffusion Restreinte ».

- A des fins de précision, **le référentiel devrait expliquer les notions de « données sensibles » et « d'informations ayant des sensibilités différentes »**[6]. Cela rendrait plus clair pour tous les acteurs la définition des niveaux de sécurité inscrite dans le référentiel et l'analyse des risques.

[6] Cf les référentiels « extérieurs », comme ceux de l'ARJEL ou de l'ASIP santé : la notion de « donnée sensible » oblige à un classement préalable des données.

5. Stockage et traitement des données en France

Il nous apparaît légitime que l'Etat impose l'hébergement sur le territoire national des données sensibles, notamment celles de son domaine de compétence régalien. Mais dans le référentiel, il conviendrait d'apporter toutes les précisions nécessaires à ce principe et à cette obligation, afin, notamment, d'être conforme avec les règles européennes de libre circulation des données.

En effet, l'exigence imposant que « le stockage et le traitement des données doivent être opérés en France[7] » peut laisser à penser que le stockage peut être à l'étranger, tandis que l'administration du système devrait être opérée en France.

- **Il conviendrait de clarifier dans le référentiel l'usage du terme « opérés » en France** dans le point 5.3.e .

- Pour tout ce qui ne concerne pas le périmètre régalien strict**, il serait nécessaire que le référentiel soit conforme au principe de libre circulation des données en Europe tel que prévu par la directive 95/46/CE** du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

- En dehors du périmètre régalien strict, en complément de la référence aux standards ISO/IEC cités plus haut, il serait particulièrement souhaitable que l'ANSSI soutienne le principe, sur lequel l'écosystème s'accorde, que le haut niveau de garantie des droits et de contrôles conférés à l'utilisateur ou au client est le premier indicateur de la sécurité des données dans le contexte de l'informatique dans le nuage.

[7] Cf 5.3 « Politiques de sécurité », du référentiel