Synthèse du référentiel

- **Historique du référentiel**
  - De la version 1.3 à la version 3.0
- **SecNumCloud v3.0 et les normes ISO relatives au cloud**
  - Normes ISO/IEC : 17788, 17789, 27017 et 27018
- **Focus sur 50 exigences pour les prestataires (CSP)**
- **Zoom sur 4 recommandations pour les commanditaires (clients)**
  - + 2 recommandations importantes additionnelles
- **Conclusion**
  - Le référentiel SecNumCloud est-il pertinent ?
  - Quel usage peut-on en faire en tant que CSP ?
  - Quel usage peut-on en faire en tant que Client ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité
des systèmes d'information

Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (*cloud computing*) - référentiel d'exigences

Version 1.3 du 30/07/2014

HISTORIQUE

- **Version 1.3 – Publiée le 30/07/2014**
  - Appel à commentaires
  - Clôture de réception des commentaires le 3/11/2014
  - 2 niveaux définis dans le même document :
    - élémentaire & standard
- **Version 2.0 – 20/03/2015 - Non publiée**
  - Version intermédiaire utilisée pour la procédure expérimentale
    - Secure Cloud & Secure Cloud plus
- **Version 3.0 – Publiée le 08/12/2016**
  - 2 niveaux définis dans 2 documents distincts :
    - SecNumCloud – niveau essentiel
    - SecNumCloud – niveau avancé

La version 1.3 ressemblait à une « mauvaise » adaptation de la norme ISO 27002 à la sécurité dans le cloud computing

- Liste d'exigences génériques peu adaptée aux contrats de cloud computing
- Très peu de distinction entre les différents prestataires (IaaS, PaaS et SaaS) malgré les différences fondamentales en matière de sécurité et de responsabilités entre prestataires et clients
- Exigences liées au chiffrement des données trop restrictives
  - Obligation d'utiliser des solutions de chiffrement qualifiées ANSSI
- Aucun niveau minimum de disponibilité exigé
- Aucune exigence en matière de réversibilité
- Exigence de localisation des données sur le territoire français : remise en cause du principe de libre circulation des données et des services au sein du marché intérieur de l'UE
- Beaucoup d'exigences spécifiques au Cloud absentes du référentiel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de services d'informatique en nuage (SecNumCloud)

référentiel d'exigences – niveau Essentiel

Version 3.0 du 8 décembre 2016

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
30/07/2014	1.3	*Version publiée pour commentaires.*	ANSSI
20/03/2015	2.0	*Version intermédiaire utilisée pour la procédure expérimentale*	ANSSI
08/12/2016	3.0	*Première version applicable.* Modifications principales : • création d'un référentiel par niveau de qualification ; • clarifications apportées à certaines exigences ; • refonte des chapitres 9, 10, 13 et des annexes ; • intégration plus précise des labels PASSI, PRIS et PDIS.	ANSSI

Publié le 8 décembre 2016 :

SecNumCloud - niveau essentiel

Définit "*un niveau de sécurité permettant le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le client*" (§ 4.1)

→ 225 exigences - 15 domaines

Publié prochainement :

SecNumCloud - niveau avancé

Définit "*un niveau de sécurité permettant le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence importante pour le client, voire pourrait mettre en péril sa pérennité*" (§ 4.2)

Source : ANSSI - *https://www.ssi.gouv.fr*

La version 1.3 du référentiel s'appuyait sur la norme ISO 27002 particulièrement inadaptée aux problématiques de sécurité dans le Cloud, la version 3.0 fait-elle référence aux nouvelles normes ISO relatives au Cloud ?

§ 1.1.1 « *Le présent référentiel s'appuie notamment sur la norme internationale ISO27001 dont il reprend d'ailleurs la structure de l'annexe A* »

- **Norme ISO/IEC 17788:2014**
  - *Informatique en nuage - Vue d'ensemble et vocabulaire*
- **Norme ISO/IEC 17789:2014**
  - *Informatique en nuage - Architecture de référence*
- **Norme 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*
- **Norme ISO/IEC 27017:2015**
  - *Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*

- 1 Scope
- 2 Normative references
  - 2.1 Identical Recommendations | International Standards
  - 2.2 Additional References
- 3 Definitions and abbreviations
  - 3.1 Terms defined elsewhere
  - 3.2 Abbreviations
- 4 Cloud sector-specific concepts
  - 4.1 Overview
  - 4.2 Supplier relationships in cloud services
  - 4.3 Relationships between cloud service customers and cloud service providers
  - 4.4 Managing information security risks in cloud services
  - 4.5 Structure of this standard
- 5 Information security policies
  - 5.1 Management direction for information security
- 6 Organization of information security
  - 6.1 Internal organization
  - 6.2 Mobile devices and teleworking
- 7 Human resource security
  - 7.1 Prior to employment
  - 7.2 During employment
  - 7.3 Termination and change of employment
- 8 Asset management
  - 8.1 Responsibility for assets
  - 8.2 Information classification
  - 8.3 Media handling
  - 9 Access control
  - 9.1 Business requirements of access control
  - 9.2 User access management
  - 9.3 User responsibilities
  - 9.4 System and application access control
- 10 Cryptography
  - 10.1 Cryptographic controls
- 11 Physical and environmental security
  - 11.1 Secure areas
  - 11.2 Equipment
- 12 Operations security
  - 12.1 Operational procedures and responsibilities
  - 12.2 Protection from malware
  - 12.3 Backup
  - 12.4 Logging and monitoring
  - 12.5 Control of operational software
  - 12.6 Technical vulnerability management
  - 12.7 Information systems audit considerations
- 13 Communications security
  - 13.1 Network security management
  - 13.2 Information transfer
- 14 System acquisition, development and maintenance
  - 14.1 Security requirements of information systems
  - 14.2 Security in development and support processes
  - 14.3 Test data
- 15 Supplier relationships
  - 15.1 Information security in supplier relationships
  - 15.2 Supplier service delivery management
- 16 Information security incident management
  - 16.1 Management of information security incidents and improvements
- 17 Information security aspects of business continuity management
  - 17.1 Information security continuity
  - 17.2 Redundancies
- 18 Compliance
  - 18.1 Compliance with legal and contractual requirements
  - 18.2 Information security reviews
- Annexes
  - A – Cloud service extended control set
  - B – References on information security risk related to cloud computing
  - Bibliography

225 exigences pour les fournisseurs Cloud (CSP)

GESTION DES ACTIFS (8)

CONTROLE D'ACCES ET GESTION DES IDENTITES (32)

SECURITE DES RESSOURCES HUMAINES (10)

CRYPTOLOGIE (14)

ORGANISATION DE LA SECURITE DE L'INFORMATION (9)

SECURITE PHYSIQUE ET ENVIRONNEMENTALE (33)

POLITIQUES DE SECURITE ET GESTION DU RISQUE (13)

SECURITE LIEE A L'EXPLOITATION (32)

EXIGENCES SUPPLEMENTAIRES (21)

(niveau essentiel)

SECURITE DES COMMUNICATIONS (8)

CONFORMITE (8)

ACQUISITION, DEVELOPPEMENT, MAINTENANCE (12)

CONTINUITE D'ACTIVITE (5)

RELATIONS AVEC LES TIERS (8)

GESTION DES INCIDENTS SECURITE (12)

mais aussi 7 recommandations à destination des commanditaires (Annexe 2)

Quels sont les prestataires qualifiés à ce jour ?

PRESTATAIRES DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ QUALIFIÉS

A ce jour, aucun prestataire n'est qualifié.

Données actualisées via le site de l'ANSSI en date du 28 janvier 2017

PRESTATAIRES DE SERVICE D'INFORMATIQUE EN NUAGE EN COURS DE QUALIFICATION

Seuls apparaissent les projets de qualification que les prestataires ont accepté de rendre publiques. En cas de suspension du projet, celui-ci est retiré de la liste.

Prestataire	Service(s)	Niveau de qualification visé	Localisation
OODRIVE	**iExtranet, PostFiles et BoardNox** Solutions de partage de fichiers et de travail collaboratif	Avancé	France
ORANGE CLOUD for BUSINESS	**Flexible Storage** Solution de synchronisation et de partage de documents, sauvegarde de données de postes de travail ou serveurs et machines virtuelles	Essentiel	France
VENDOME SOLUTIONS	**IaaS avec Plan de Reprise d'Activité** Hébergement et gestion de centre de données	Avancé	France

Source : ANSSI - *https://www.ssi.gouv.fr*

SecNumCloud
(niveau essentiel)

Focus sur 50 exigences à destination des CSP

- Une exigence → mesures de sécurité à mettre en œuvre par le CSP
  - Les mesures de sécurité qui s'ajoutent ou qui précisent des mesures de référentiels existants :
    - Norme ISO/IEC 27002:2013 - *(114 security controls)*
    - Norme ISO/IEC 27017:2015 - *(44 security controls)*
    - Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) - *(136 security controls)*
  - Interrogations habituelles pour les clients de service Cloud

5 - POLITIQUE DE SECURITE DE L'INFORMATION ET GESTION DU RISQUE

- 5.1. Principes (2)
- 5.2. Politique de sécurité de l'information (5)
- 5.3. Appréciation des risques (6)

13 exigences

- Le CSP doit appliquer le guide d'hygiène informatique de l'ANSSI [HYGIENE].
- Le CSP doit réaliser une appréciation des risques. Cette appréciation des risques doit notamment prendre en compte la gestion des informations clients, les risques de défaillance des mécanismes de cloisonnement, les risques liés à l'effacement incomplet ou non sécurisé sur des supports partagés ainsi que les risques liés aux obligations légales et règlementaires.

6 - ORGANISATION DE LA SECURITE DE L'INFORMATION

- 6.1. Fonctions et responsabilités liées à la sécurité de l'information (4)
- 6.2. Séparation des tâches (1)
- 6.3. Relations avec les autorités (1)
- 6.4. Relations avec les groupes de travail spécialisés (1)
- 6.5. La sécurité de l'information dans la gestion de projet (2)

9 exigences

- Le CSP doit faire une analyse de risques préalable pour tout projet pouvant impacter le service Cloud et informer le client par écrit des impacts potentiels, des mesures mises en place et des risques résiduels.

7 - SECURITE DES RESSOURCES HUMAINES

- 7.1. Sélection des candidats (1)
- 7.2. Conditions d'embauche (3)
- 7.3. Sensibilisation, apprentissage et formations à la sécurité de l'information (3)
- 7.4. Processus disciplinaire (2)
- 7.5. Rupture, terme ou modification du contrat de travail (1)

10 exigences

- Sur demande d'un client, le CSP doit fournir son règlement intérieur et la charte d'éthique.
- Le CSP doit documenter et mettre en œuvre un processus disciplinaire applicable à l'ensemble du personnel en cas de violation de la PSSI.
- Sur demande d'un client, le CSP doit communiquer les sanctions encourues par le personnel.

8 - GESTION DES ACTIFS

- 8.1. Inventaire et propriété des actifs (3)
- 8.2. Restitution des actifs (1)
- 8.3. Identification des besoins de sécurité de l'information (2)
- 8.4. Marquage et manipulation de l'information (0)
- 8.5. Gestion des supports amovibles (2)

8 exigences

- Le CSP doit documenter et mettre en œuvre une procédure de restitution des actifs.
- Lorsque le client confie au CSP des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques, le CSP doit identifier les besoins de sécurité spécifiques associés à ces contraintes.

9 - CONTROLE D'ACCES ET GESTION DES IDENTITES

- 9.1. Politiques et contrôle d'accès (2)
- 9.2. Enregistrement et désinscription des utilisateurs (3)
- 9.3. Gestion des droits d'accès (7)
- 9.4. Revue des droits d'accès utilisateurs (3)
- 9.5. Gestion des authentifications des utilisateurs (4)
- 9.6. Accès aux interfaces d'administration (10)
- 9.7. Restriction des accès à l'information (3)

32 exigences

- Le CSP doit être en mesure de fournir, pour une ressource donnée, la liste de tous les droits d'accès attribués aux utilisateurs qu'ils soient sous la responsabilité du CSP ou du client.
- Pour un service SaaS, le CSP doit proposer à minima une option d'authentification à deux facteurs pour les utilisateurs finaux.
- Le CSP doit mettre en place un système d'authentification à double facteur pour l'accès à toutes les interfaces administrateurs (CSP et clients).
- Pour un service SaaS, l'interface d'administration mises à disposition des clients doit être séparée de l'interface d'accès des utilisateurs finaux.

10 - CRYPTOLOGIE

- 10.1. Chiffrement des données stockées (3)
- 10.2. Chiffrement des flux (4)
- 10.3. Hachage des mots de passe (3)
- 10.4. Non répudiation (1)
- 10.5. Gestion des secrets (3)

14 exigences

- Le CSP doit chiffrer les données des clients pour empêcher la récupération de données en cas de réallocation d'une ressource ou de récupération d'un support physique (*§* 10.1.a)
- Le CSP doit mettre en œuvre les règles définies dans les annexes B1 et B2 du RGS [CRYPTO_B1] et [CRYPTO_B2].
- Concernant le chiffrement des flux réseaux, le CSP doit appliquer les recommandations de l'ANSSI à savoir : [NT_TLS] pour TLS, [NT_IPSEC] pour IPSec et [NT_SSH] pour SSH.
- Le CSP doit protéger l'accès aux clés cryptographiques via un conteneur (logiciel ou matériel) ou un support disjoint.

11 - SECURITE PHYSIQUE ET ENVIRONNEMENTALE

- 11.1. Périmètres de sécurité physique (2)
- 11.2. Contrôle d'accès physique (14)
- 11.3. Protection contre les menaces extérieures et environnementales (5)
- 11.4. Travail dans les zones privées et sensibles (2)
- 11.5. Zones de livraison et de chargement (1)
- 11.6. Sécurité du câblage (2)
- 11.7. Maintenance des matériels (4)
- 11.8. Sortie des actifs (1)
- 11.9. Recyclage sécurisé du matériel (1)
- 11.10. Matériel en attente d'utilisation (1)

33 exigences

- Le CSP doit s'assurer que les supports ne peuvent être retournés à un tiers que si les données du client y sont stockées chiffrées ou ont préalablement été détruites à l'aide d'un mécanisme d'effacement sécurisé par réécriture de motifs aléatoires *(exigence § 11.7.c en contradiction avec § 10.1.a)*.
- Le CSP doit documenter et mettre en oeuvre des moyens permettant d'effacer de manière sécurisée par réécriture de motifs aléatoires tout support de données mis à disposition d'un client *(exigence § 11.9.a en contradiction avec § 10.1.a)*. Si l'espace de stockage est chiffré, l'effacement peut être réalisé par un effacement sécurisé de la clé de chiffrement.

12 - SECURITE LIEE A L'EXPLOITATION

- 12.1. Procédures d'exploitation documentées (1)
- 12.2. Gestion des changements (4)
- 12.3. Séparation env. de dév., test et exploitation (1)
- 12.4. Mesures contre les codes malveillants (2)
- 12.5. Sauvegarde des informations (4)
- 12.6. Journalisation des événements (4)
- 12.7. Protection de l'information journalisée (5)
- 12.8. Synchronisation des horloges (2)
- 12.9. Analyse et corrélation des événements (2)
- 12.10. Installation de logiciels (2)
- 12.11. Gestion des vulnérabilités techniques (2)
- 12.12. Administration (3)

32 exigences

- Dans le cadre d'un service SaaS, le CSP doit informer au plus tôt le client de toute modification à venir sur les éléments du service dès lors qu'elle est susceptible d'occasionner une perte de fonctionnalité pour le client.
- Les sauvegardes sont assujetties aux mêmes exigences de localisation que les données opérationnelles. Le ou les sites de sauvegarde sont assujettis aux mêmes exigences de sécurité que le site principal.
- Le CSP doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires. Le CSP doit fournir, sur demande d'un client, l'ensemble des événements le concernant.
- Le CSP doit documenter et mettre en oeuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité du système d'information du service, en temps réel ou *a posteriori* pour des événements remontant jusqu'à six mois.

13 - SECURITE DES COMMUNICATIONS

- 13.1. Cartographie du système d'information (2)
- 13.2. Cloisonnement des réseaux (5)
- 13.3. Surveillance des réseaux (1)

8 exigences

- Le CSP doit établir et tenir à jour une cartographie du système d'information du service comprenant la matrice des flux réseau autorisés en précisant pour chaque flux sa description technique (services, protocoles et ports) et sa justification métier ou d'infrastructure.
- Le CSP doit cloisonner, physiquement ou par chiffrement, tous les flux de données internes au système d'information du service vis-à-vis de tout autre système d'information.
- Le CSP doit mettre en place et configurer un pare-feu applicatif pour protéger les interfaces d'administration destinées à ses clients et exposées sur un réseau public.

14 - ACQUISITION, DEVELOPPEMENT, MAINTENANCE DES SYSTEMES D'INFORMATION

- 14.1. Politique de développement sécurisé (2)
  14.2. Procédures de contrôle des changements de système (3)
- 14.3. Revue technique des applications après changement apporté à la plateforme d'exploitation (1)
- 14.4. Environnement de développement sécurisé (2)
- 14.5. Développement externalisé (1)
- 14.6. Test de la sécurité et conformité du système (1)
- 14.7. Protection des données de test (2)

12 exigences

- Le CSP doit mettre en oeuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.
- Si le CSP souhaite utiliser des données client issues de la production pour réaliser des tests, il doit préalablement obtenir l'accord du client et les anonymiser. Le CSP doit assurer la confidentialité des données lors de leur anonymisation.

15 - RELATIONS AVEC LES TIERS

- 15.1. Identification des tiers (1)
- 15.2. La sécurité dans les accords conclus avec les tiers (3)
- 15.3. Surveillance et revue des services des tiers (1)
- 15.4.Gestion des changements apportés dans les services des tiers (2)
- 15.5.Engagements de confidentialité (1)

8 exigences

- Le CSP doit exiger des tiers participant à la mise en oeuvre du service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Le CSP doit inclure ces exigences dans les contrats conclus avec les tiers.
- Le CSP doit contractualiser, avec chacun des tiers participant à la mise en oeuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent référentiel.

16 - GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

- 16.1. Responsabilités et procédures (2)
- 16.2. Signalements liés à la sécurité de l'information (4)
- 16.3. Appréciation des événements liés à la sécurité de l'information et prise de décision (2)
- 16.4. Réponse aux incidents liés à la sécurité de l'information (2)
- 16.5. Tirer des enseignements des incidents liés à la sécurité de l'information (1)
- 16.6. Recueil de preuves (1)

12 exigences

- Le CSP doit documenter et mettre en oeuvre une procédure permettant à l'ensemble des clients de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.
- Le CSP doit communiquer sans délai aux clients les incidents de sécurité et les préconisations associées pour en limiter les impacts. Il doit permettre au client de choisir les niveaux de gravité des incidents pour lesquels il souhaite être informé.
- Le CSP doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents de sécurité. Pour l'appréciation, il doit s'appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec le client.
- Le CSP doit documenter et mettre en oeuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.

17 - CONTINUITE D'ACTIVITE

- 17.1. Organisation de la continuité d'activité (2)
- 17.2. Mise en oeuvre de la continuité d'activité (1)
- 17.3. Vérifier, revoir et évaluer la continuité d'activité (1)
- 17.4. Disponibilité des moyens de traitement de l'information (1)

5 exigences

- Le CSP doit documenter et mettre en oeuvre des procédures permettant de maintenir ou de restaurer l'exploitation du service et d'assurer la disponibilité des informations au niveau et dans les délais pour lesquels il s'est engagé vis-à-vis du client dans la convention de service.
- Le CSP doit documenter et mettre en oeuvre les mesures qui lui permettent de répondre au besoin de disponibilité du service défini dans la convention de service.

18 - CONFORMITE

- 18.1. Identification de la législation et des exigences contractuelles applicables (4)
- 18.2. Revue indépendante de la sécurité de l'information (2)
- 18.3. Conformité avec les politiques et les normes de sécurité (1)
- 18.4. Examen de la conformité technique (1)

8 exigences

- Le CSP doit identifier les exigences légales, réglementaires et contractuelles en vigueur applicables au service. En France, le CSP doit considérer au minimum les textes suivants : les données à caractère personnel, le secret professionnel, l'abus de confiance, le secret des correspondances privées, l'atteinte à la vie privée et l'accès ou le maintien frauduleux à un système d'information.
- Le CSP doit documenter et mettre en oeuvre les procédures permettant de respecter les exigences légales, réglementaires et contractuelles en vigueur ainsi que les besoins de sécurité spécifiques.
- Le CSP doit, sur demande d'un client, lui rendre accessible l'ensemble de ces procédures.
- Le CSP doit documenter et mettre en oeuvre un programme d'audit sur trois ans définissant le périmètre et la fréquence des audits.
- Le CSP doit inclure dans le programme d'audit un audit qualifié par an réalisé par un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié.
- Le CSP doit documenter et mettre en oeuvre une politique permettant de vérifier la conformité technique du service aux exigences du référentiel SecNumCloud. Cette politique doit définir les objectifs, méthodes, fréquences, résultats attendus et mesures correctrices.

19 - EXIGENCES SUPPLEMENTAIRES

- 19.1. Convention de service (13)
- 19.2. Localisation des données (4)
- 19.3. Régionalisation (2)
- 19.4. Fin de contrat (2)

21 exigences

- Le CSP doit établir une convention de service avec chacun des clients du service dans laquelle il doit identifier : les responsabilités de chacune des parties (clients, CSP, tiers), les éléments explicitement exclus des responsabilités du CSP ainsi que la localisation du service.
- Le CSP doit inclure dans la convention de service une clause de réversibilité permettant au client de récupérer l'ensemble de ses données.
- Le CSP doit assurer cette réversibilité soit via la mise à disposition de fichiers dans un format documenté et exploitable en dehors du service fourni par le CSP soit par la mise en place d'interfaces techniques permettant l'accès aux données suivant un schéma documenté et exploitable. Les modalités techniques de la réversibilité doivent figurer dans la convention de service.
- Le CSP doit indiquer dans la convention de service qu'il ne peut se prévaloir de la propriété des données transmises et générées par le client. Ces données relèvent de la propriété du client.

21 exigences (suite)

- Le CSP doit préciser dans la convention de service que :
  - le service est qualifié et inclure l'attestation de qualification
  - le client peut déposer une réclamation relative au service qualifié auprès de l'ANSSI
  - le client autorise l'ANSSI et l'organisme de qualification à auditer le service et son SI relatif au service afin de vérifier qu'ils respectent les exigences du référentiel SecNumCloud
  - Le client autorise un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié mandaté par le CSP à auditer le service et son système d'information dans le cadre du plan de contrôle
- Le CSP doit proposer une convention de service appliquant le droit d'un État membre de l'UE.
- Le CSP doit stocker et traiter les données du client au sein de l'UE.
- Les opérations d'administration et de supervision du service doivent être réalisées depuis l'UE, cependant les opérations de support aux clients peuvent s'effectuer depuis un État hors de l'UE.
- Au terme du contrat le CSP doit assurer un effacement sécurisé de l'intégralité des données du client. L'effacement doit être réalisé dans un délai précisé dans la convention de service par la réécriture complète de tout support ayant hébergé les données du client ou l'effacement des clés utilisées pour le chiffrement des espaces de stockage du client.
- A la fin du contrat, le CSP doit supprimer toutes les données techniques relatives au client (annuaire, certificats, configuration des accès, ...).

Annexe 2 : 7 recommandations aux commanditaires

- Si le commanditaire est une autorité administrative (AA) ou un opérateur d'importance vitale (OIV), il peut demander à l'ANSSI de participer à la définition du cahier des charges faisant l'objet d'un appel d'offres ou d'un contrat.
- Il est recommandé que le commanditaire choisisse son CSP dans le catalogue des CSPs qualifiés publié sur le site de l'ANSSI, la qualification d'un CSP d'informatique en nuage attestant de sa conformité à l'ensemble des exigences du présent référentiel.
- Pour bénéficier d'une prestation qualifiée (i.e. conforme à l'ensemble des exigences du référentiel SecNumCloud), le commanditaire doit non seulement choisir le CSP dans le catalogue des CSPs qualifiés publié sur le site de l'ANSSI mais également exiger du CSP de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée. En effet, un CSP qualifié garde la faculté de réaliser des prestations non qualifiées. Le recours à un CSP issu du catalogue des CSPs qualifiés est donc une condition nécessaire mais pas suffisante pour bénéficier d'une prestation qualifiée. Le commanditaire doit donc exiger explicitement une prestation qualifiée.
- Le commanditaire peut déposer auprès de l'ANSSI une réclamation contre un CSP qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée. S'il s'avère après instruction de la réclamation que le CSP n'a pas respecté une ou plusieurs exigences du référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du CSP peut être suspendue, retirée ou sa portée de qualification réduite.

Les 2 recommandations supplémentaires de VeriSafe

- Toute exigence qui ne peut être vérifiée lors de la qualification doit faire l'objet d'une clause explicite dans la convention de service signée avec le fournisseur.
  - Si le service est qualifié SecNumCloud, il ne devrait y avoir aucune raison pour qu'un fournisseur refuse d'intégrer dans le contrat une clause qui résulte directement d'une des 225 exigences du référentiel.

- Choisir un CSP qualifié ne suffit pas pour assurer la sécurité des données. Les clients ne doivent pas oublier de faire tout ce que le fournisseur ne fera **JAMAIS** pour eux :
  - Classifier les données
  - Identifier les contraintes légales, réglementaires ou sectorielles spécifiques
  - Identifier les mesures de sécurité qui incombent au client (ISO 27017, CCM)
  - Assurer la sécurité des postes utilisateurs
  - Sensibiliser les utilisateurs pour un usage sécurisé des services
  - Compléter le cas échéant la sécurité du CSP par des solutions CASB
  - Compléter les pénalités insuffisantes des CSP par une couverture assurantielle
  - Valider la sécurité par une analyse de risques simplifiée (matrice MERC) ou via la méthodologie EFICAS

Conclusion

- **Le référentiel SecNumCloud est-il pertinent ?**
  - Quelles sont ses limites ou insuffisances ?
- **Quel usage peut-on en faire en tant que CSP ?**
  - Respecter toutes les exigences pour être qualifié officiellement par l'ANSSI et gagner ainsi la confiance des clients
  - Respecter tout ou partie du référentiel pour améliorer la sécurité du service et diminuer en particulier les risques juridiques et d'image
- **Quel usage peut-on en faire en tant que client ?**
  - Identifier et choisir un CSP qualifié (en conformité avec les 225 exigences du référentiel)
  - Disposer de garanties sur les engagements du CSP
  - Diminuer les risques financiers, juridiques et d'image
  - Utilisation en tant que guide de bonnes pratiques
    - Sélection des exigences pertinentes dans le contexte du client
    - Soumission au CSP sous forme d'un questionnaire
    - Analyse des réponses du CSP pour vérifier la conformité aux exigences
    - Exemple chez Verisafe : 225 exigences SecNumCloud dans la matrice MERC et questionnaire intégré dans les outils de la méthodologie EFICAS.