



OBSERVATOIRE

SecNumCloud

ÉDITION MARS 2026



SecNumCloud: un pilier de notre souveraineté numérique

Par **Anne Le Hénaff**

**Ministre déléguée chargée
de l'Intelligence Artificielle
et du Numérique**

À l'heure où les menaces cyber s'intensifient et où l'application de cadres juridiques extra-européens à portée extra-territoriale fait peser un risque réel sur la maîtrise de nos données, la question de la confiance dans le numérique est devenue centrale.

C'est pourquoi le Gouvernement s'est engagé, à travers la stratégie nationale pour le cloud, à instaurer un cadre réglementaire protecteur et à soutenir l'émergence d'un marché du cloud de confiance. SecNumCloud incarne cette ambition : un référentiel de sécurité exigeant, conçu pour garantir la protection des systèmes d'information face aux cyberattaques et préserver la confidentialité des données les plus sensibles.

L'accroissement du nombre d'offres labellisées par l'ANSSI constitue une excellente nouvelle. Il témoigne de la maturité croissante de l'écosystème et de sa capacité à répondre aux besoins de plus en plus diversifiés des administrations et des entreprises. La multiplication des offres permet aujourd'hui d'accompagner un nombre croissant de cas d'usage, avec davantage d'applications, de services et de niveaux de performance, sans compromis sur les exigences de sécurité.

Cette dynamique est essentielle pour réussir la migration vers le cloud, levier clé de modernisation des systèmes d'information. Elle démontre qu'il est possible d'accélérer la transformation numérique, de gagner en agilité et en efficacité, tout en maintenant un haut niveau de protection des données.

C'est pourquoi je salue le travail mené par la Cyber Task Force dans le cadre de cet observatoire. Cette production contribue à la valorisation des acteurs qui ont fait le choix exigeant de s'inscrire dans le processus de qualification SecNumCloud. L'observatoire SecNumCloud permet de rendre visible les efforts consentis par les fournisseurs en matière de sécurité, de gouvernance et de conformité. Ce travail de pédagogie et de mise en lumière est essentiel pour rappeler que la confiance numérique n'est ni abstraite ni automatique, mais le fruit d'un engagement durable et exigeant.

À l'heure où l'Europe prépare de nouveaux cadres réglementaires, notamment dans le domaine du cloud et de l'intelligence artificielle, la France peut s'appuyer sur cet Observatoire SecNumCloud pour rappeler avec constance qu'un schéma de certification européen est indispensable pour protéger nos données sensibles et garantir notre souveraineté numérique face aux législations extraterritoriales. Lors du Sommet sur la souveraineté numérique de Berlin en novembre 2025, la France et l'Allemagne se sont déjà accordés sur une définition du cloud souverain qui exclut les services portant des risques sur l'extraterritorialité des données. Cette convergence constitue une première étape, appelée à être consolidée au niveau européen.

***Ensemble,
portons ce combat pour
la souveraineté numérique !***

SecNumCloud

c'est quoi ?

SecNumCloud est le référentiel de l'ANSSI qui définit les exigences de sécurité et de souveraineté pour les services d'informatique en nuage (cloud) utilisés par les administrations et entreprises en France.

La différence entre qualification et certification

La qualification vérifie l'aptitude d'un prestataire ou d'un service à répondre à un besoin (confiance, compétences, niveau attendu).

La certification atteste officiellement, via un organisme tiers, la conformité à une norme ou un référentiel précis.



Il vise à attester

- 1 de la qualité et de la robustesse d'un service cloud
- 2 de la compétence de l'opérateur de cloud
- 3 ainsi que de la confiance pouvant lui être accordée

Il établit un cadre

- 1 technique
- 2 opérationnel
- 3 juridique



Critères Techniques

- > **Appréciation des risques** documentée couvrant l'ensemble du périmètre du service
- > **Révision annuelle** des plans de sécurité de l'information et de continuité d'activité
- > **Obligation d'information** du commanditaire en cas de violation de données à caractère personnel
- > **Désignation** d'un responsable de la sécurité des systèmes d'information
- > **Désignation** d'un responsable de la sécurité physique
- > **Politique de sauvegarde** quotidienne des données



Critères Opérationnels

- > **Authentification multifacteurs** fort pour l'accès aux interfaces d'administration
- > **Comptes nominatifs** pour les utilisateurs
- > **Mécanisme de chiffrement** empêchant la récupération de données lors de la réallocation d'une ressource ou d'un support physique
- > **Cloisonnement des flux** réseau (logique/physique/chiffré)
- > **Veille active** pour gérer les vulnérabilités techniques, évaluer l'exposition aux risques



Critères Juridiques

- > **Doivent être établis au sein d'un État membre de l'UE** : le siège statutaire, l'administration centrale et le principal établissement du prestataire
- > **Limites sur la détention du capital** et des droits de vote par des entités hors UE: 24% individuellement, 39% collectivement
- > **Stockage et traitement des données au sein de l'UE**
- > **Justification du respect des principes du RGPD** (finalités légitimes, durée de conservation des données limitée)
- > **Une clause de réversibilité** doit être contenue dans la convention de service prévoyant la restitution et l'effacement sécurisé des données du commanditaire en fin de contrat ou pour toute autre cause



La procédure de qualification

- | | | | |
|-----------|--|-----------|---------------------------------------|
| J0 | Demande de qualification auprès de l'ANSSI | J2 | Travaux d'évaluation acceptés |
| J1 | Stratégie d'évaluation acceptée | J3 | Décision de qualification par l'ANSSI |



- | | | | |
|---|--|--|---|
| <ul style="list-style-type: none"> > Description détaillée des services soumis à qualification > Démonstration de la conformité au référentiel SecNumCloud > Choix d'un auditeur qualifié chargé de mener les audits J2 | <ul style="list-style-type: none"> > Validation par l'ANSSI du plan d'audit proposé par l'organisme d'évaluation > Fixation de la feuille de route des audits J2 | <ul style="list-style-type: none"> > Audits techniques et organisationnels sur site par l'organisme agréé > Transmission du rapport à l'ANSSI pour analyse | <ul style="list-style-type: none"> > Étude du rapport d'audit J2 par l'ANSSI > Demande d'éventuelles actions correctives par l'ANSSI > Potentielle demande de compléments d'information ou validation de la certification |
|---|--|--|---|

Les principaux critères d'évaluation



Critères Techniques

- > **Appréciation des risques** documentée couvrant l'ensemble du périmètre du service
- > **Établissement et actualisation annuelle** des plans de sécurité de l'information et de continuité d'activité
- > **Obligation d'information** du commanditaire en cas de violation de données à caractère personnel
- > Désignation d'un **responsable de la sécurité des systèmes d'information**
- > Désignation d'un **responsable de la sécurité physique**
- > Politique de **sauvegarde quotidienne des données**



Critères Opérationnels

- > **Authentification multifacteurs fort** pour l'accès aux interfaces d'administration
- > **Comptes nominatifs** pour les utilisateurs
- > **Mécanisme de chiffrement** empêchant la récupération lors d'une réallocation de ressource ou d'un support physique
- > **Cloisonnement des flux réseau** (logique/physique/chiffré)
- > **Veille active** pour gérer les vulnérabilités techniques, évaluer l'exposition aux risques



Critères Juridiques

- > Le siège statutaire, l'administration centrale et le principal établissement du prestataire doivent être établis au sein d'un État membre de l'UE
- > Limites sur la détention du capital et des droits de vote par des entités hors UE:
24% individuellement, 39% collectivement
- > Stockage et traitement des données au sein de l'UE
- > Respect des principes du RGPD justifié (finalités légitimes, durée de conservation limitée)
- > La convention de service doit inclure une clause de réversibilité prévoyant la restitution et l'effacement sécurisé des données du commanditaire en fin de contrat ou pour toute autre cause

SecNumCloud

c'est qui ?

Les services soumis à la qualification

	EN COURS		LES QUALIFIÉS	
	Candidat	Offre	Entreprises	Offre
IaaS	Adista Bleu Cyllene ITS Ecritel Gip Mipih (Numih France) ITS Integra Numspot Orange Business OVH SAS Proival - Groupe Tenexa Scaleway Bretagne Télécom	dista Secure Cloud Cloud de Confiance Bleu IaaS SecNumCloud Ecritel Secure Cloud Cloud Premier Souverain IT SecureCloud Plateforme des services cloud Cloud Avenue SecNum Dynamic SNC Cloud Platform Horizon SecNumCloud Scaleway SecNumCloud Blue Secure Cloud	Cegedim Cloud Temple OVH OVH Orange Business Outscale Worldline S3NS	CegNumCloud Secured IaaS IAAS Secure Temple Bare Metal Pod Hosted Private Cloud powered by VMware CloudAvenueSecNum IaaS Worldline Cloud Services Cloud de Confiance PREMI3NS
CaaS	Bleu ITS Integra	Cloud de Confiance Bleu ITSecureKube	S3NS	Cloud de Confiance PREMI3NS
PaaS	Bleu OVH SAS Scaleway	Cloud de Confiance Bleu SNC Cloud Platform Scaleway SecNumCloud	Cloud Temple S3NS	PaaS Openshift Cloud de Confiance PREMI3NS
SaaS	Ecritel Solutions NetExplorer Cloud Solutions	Ecritel Secure Backup Share and Workspace Wimi	Index Education Index Education Index Education Index Education Oodrive Oodrive Oodrive Whaller	EDT Hyperplanning Pronote Pronote Primaire Oodrive_Work_Share Oodrive_Work Oodrive_Meet Whaller Donjon SaaS

Free Pro est également en cours de qualification mais aucune information publique n'est disponible sur le type de qualification demandée

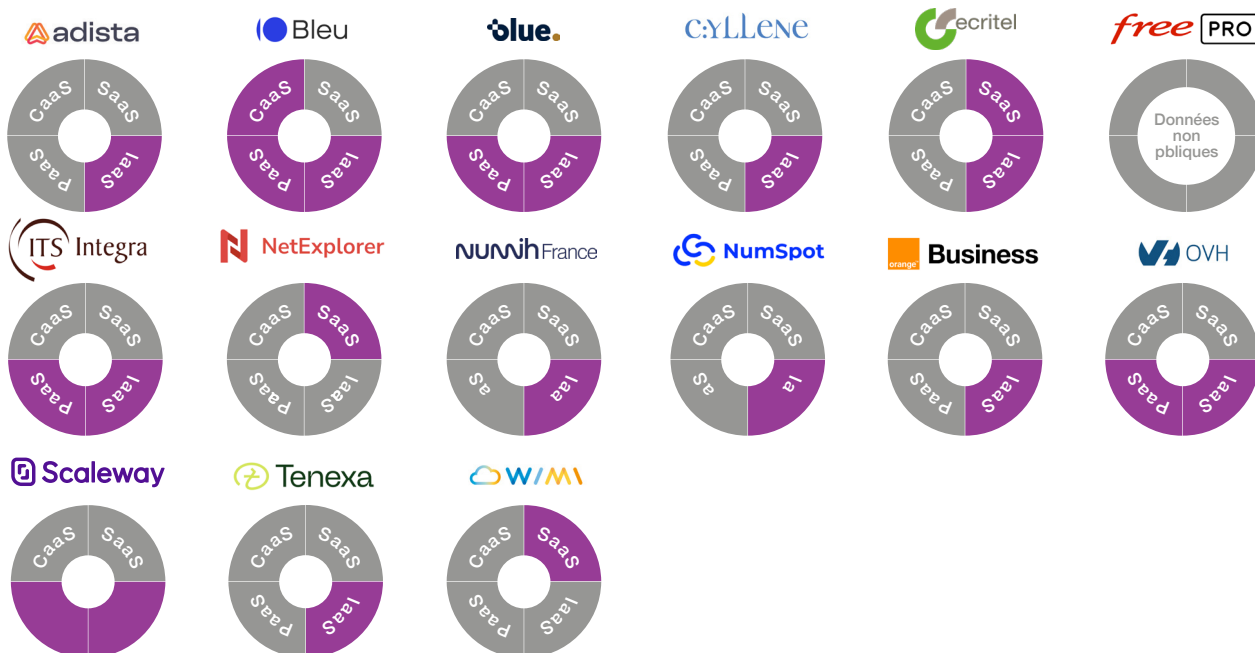
Les candidats

IaaS	adista Bleu blue. orange Business cyLLene ecritel (ITS) Integra numihFrance NumSpot OVH Scaleway Tenexa
CaaS	Bleu (ITS) Integra
PaaS	Bleu OVH Scaleway
SaaS	ecritel NetExplorer WIMI

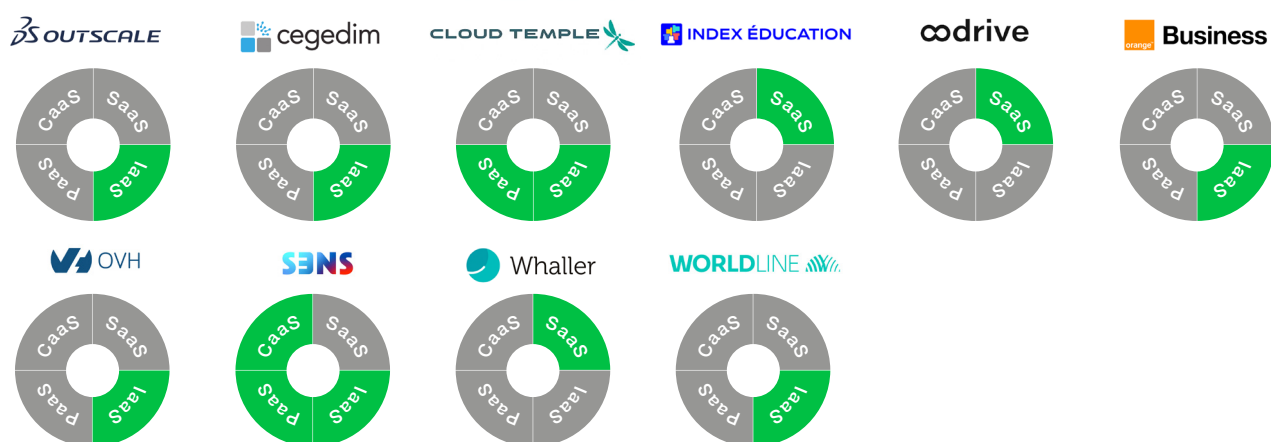


Périmètre de la qualification

EN COURS



LES QUALIFIÉS



Statut des candidats à la qualification

J0

Demande
de qualification
auprès de l'ANSSI

J1

Stratégie
d'évaluation
acceptée

J2

Travaux
d'évaluation
acceptés

J3

Décision
de qualification
par l'ANSSI



ITS Integra
Tenexa blue.
adista

Bleu ecritel
NetExplorer
NumSpot Scaleway

SENS

Lexique



IaaS (Infrastructure as a Service)

- > Mise à disposition de ressources informatiques physiques.
- > **Le prestataire détient** l'infrastructure physique et la loue/la met à disposition d'un utilisateur.
- > **Le client construit** son activité sur cette plateforme.
- > **Le prestataire** détient tout le matériel physique: les machines, le réseau et le stockage ...
- > **Le client** (commanditaire) :
 - construit les services en fonction de ses besoins
 - décide du champ d'application/périmètre
 - décide des usages rendus possibles sur l'infrastructure loué.

Les points spécifiques "IaaS"

- **Cloisonnement strict** entre les utilisateurs
- Pour empêcher la récupération des données en cas de réallocation de ressource ou de récupération du support physique => **chiffrement du disque ou du système de fichier ou chiffrement par volume avec une clé par commanditaire**

CaaS (Container as a Service)

- > Mise à disposition d'outils permettant de **déployer, gérer et orchestrer des conteneurs** d'applications.
- > **Un conteneur** est comme une petite boîte isolée qui contient tout le nécessaire pour faire fonctionner une application (bibliothèques, code, outils...), sans interférer avec les autres.
- > **Le prestataire** gère l'infrastructure sous-jacente (serveurs, stockage, réseau, système d'exploitation).
- > **Le client** (commanditaire) :
 - contrôle les conteneurs et les éléments techniques liés à ses applications.

Les points spécifiques "CaaS"

- **Cloisonnement strict** entre les commanditaires
- **Cryptologie recommandée** : chiffrement par volume une clé/commanditaire)
- **Effacement sécurisé** à la fin du contrat = effacement sécurisé des clés de chiffrement des espaces de stockage du commanditaire.
- Les opérations d'administration et de supervision doivent être réalisées depuis l'Union Européenne.

PaaS (Platform as a Service)

- > Mise à disposition d'une **plateforme technique prête à l'emploi** pour développer, héberger et faire fonctionner des applications.
- > **Le prestataire** gère toute la partie infrastructure (réseau, serveurs, stockage, système d'exploitation, etc.).
- > **Le client** (commanditaire) :
 - se concentre sur le développement et la gestion de ses propres applications.

Les points spécifiques "PaaS"

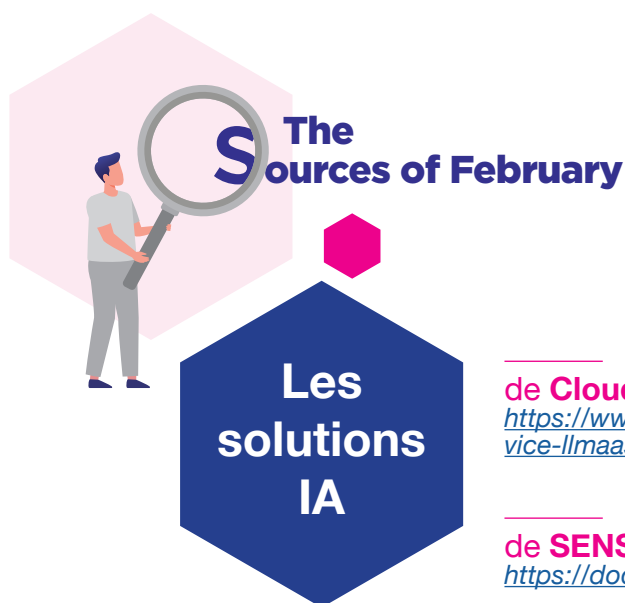
- **Devoir d'information** par le prestataire en cas de modification sur les éléments logiciels qu'il maîtrise.
- **Cloisonnement strict** entre les interfaces des commanditaires: les ressources affectées à l'usage d'un prestataire ne doivent pas être accessibles à d'autres commanditaires.

SaaS (Software as a Service)

- > Mise à disposition d'**applications prêtes à l'emploi**, hébergées dans le cloud et gérées entièrement par le prestataire.
- > L'utilisateur accède simplement à l'application via Internet — sans avoir à installer, héberger ou maintenir quoi que ce soit.
- > **Le prestataire** gère l'ensemble des aspects techniques requérant des compétences informatiques.
- > **Le client** (commanditaire) :
 - Ne maîtrise pas la plateforme en nuage.
 - Peut d'effectuer quelques paramétrages dans l'application.

Les points spécifiques "SaaS"

- **Moyens d'authentification à multiples facteurs** pour l'accès des utilisateurs finaux
- **Cloisonnement** entre les interfaces d'administration mises à disposition des commanditaires et les interfaces permettant l'accès des utilisateurs finaux



de Cloud Temple

<https://www.cloud-temple.com/en/large-language-model-as-a-service-llmaas/>

de SENS

<https://documentation.s3ns.fr/compute/docs/gpus?hl=fr#a3-series>

de Bleu

<https://www.bleucloud.fr/telechargement-liste-des-services-azure/>

de NumSpot

<https://numspot.com/produit/data-intelligence-artificielle-souveraine/>

de Orange Business Services

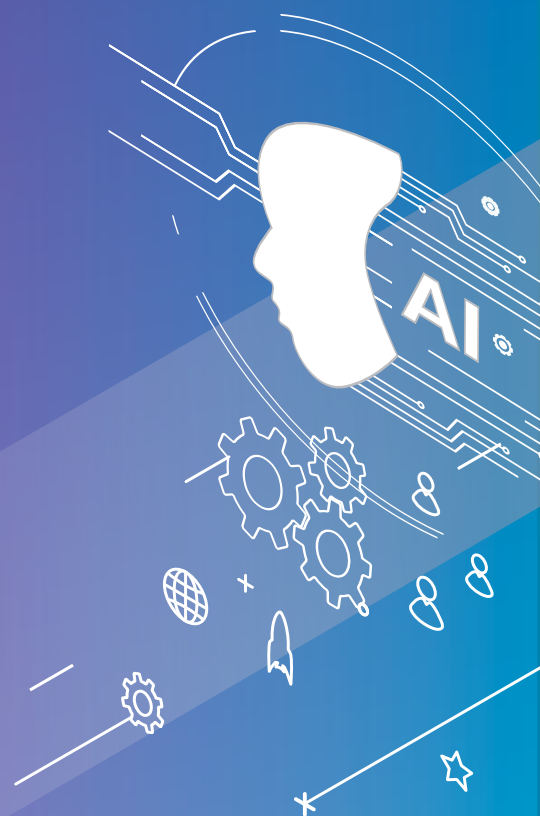
<https://www.orange.com/fr/communiques/orange-business-lance-en-france-de-nouvelles-offres-pour-mener-des-projets-dia-generative-de-bout-en-bout-et-de-confiance-232094?>

de Scaleway

<https://www.scaleway.com/en/custom-built-clusters/>

d'Outscale

<https://fr.outscale.com/cloud-experience/cloud-souverain/>



ÉDITION
MARS 2026