



OBSERVATORY

SecNumCloud

MARCH 2026 EDITION



SecNumCloud: A Pillar of Our Digital Sovereignty

By **Anne Le Hénanff**

**Minister Delegate
for Artificial Intelligence
and Digital Affairs**

At a time when cyber threats are intensifying and the extraterritorial reach of non-European legal frameworks poses a tangible risk to our control over data, trust in the digital sphere has become a central concern.

This is why the Government, through its national cloud strategy, has committed to establishing a protective regulatory framework and accompanying the emergence of a trusted cloud market. SecNumCloud embodies this ambition: a demanding security framework designed to safeguard information systems against cyberattacks and to ensure the confidentiality of our most sensitive data.

The growing number of solutions certified by Agence nationale de la sécurité des systèmes d'information (ANSSI) is excellent news. It reflects the increasing maturity of the ecosystem and its ability to meet the ever more diverse needs of public administrations and businesses. The expansion of certified offerings now makes it possible to support a wider range of use cases, with more applications, services, and performance levels—without compromising on security.

This momentum is essential to the success of cloud migration, a key lever for modernising information systems. It demonstrates that we can accelerate digital transformation, enhance agility and efficiency, and at the same time maintain a high level of data protection.

I therefore support the work carried out by the Cyber Task Force through this Observatory. This publication helps highlight and recognise the stakeholders who have made the demanding choice to commit to the SecNumCloud qualification process. The SecNumCloud Observatory brings visibility to the efforts undertaken by providers in terms of security, governance, and compliance. This work of clarification and transparency is crucial in reminding us that digital trust is neither abstract nor automatic, but the result of sustained and exacting commitment.

As Europe prepares new regulatory frameworks, particularly in the fields of cloud and artificial intelligence, France can rely on this SecNumCloud Observatory to consistently reaffirm that a European certification scheme is indispensable to protecting our sensitive data and safeguarding our digital sovereignty against extraterritorial legislation. At the Berlin Digital Sovereignty Summit in November 2025, France and Germany agreed on a definition of sovereign cloud that excludes services carrying risks linked to data extraterritoriality. This convergence marks an important first step, one that must now be consolidated at the European level.

***Together,
let us carry forward this fight
for digital sovereignty.***

SecNumCloud

What is it?

SecNumCloud is the ANSSI framework that defines security and sovereignty requirements for cloud computing services used by administrations and businesses in France.

The difference between qualification and certification

A **qualification** verifies a provider's or service's ability to meet a need (trust, skills, expected level).

A **certification**, issued by a third-party organization, attests to conformity with a specific standard or framework.



It aims to attest

- 1 The quality and robustness of a cloud service
- 2 The competence of the cloud operator
- 3 The trust that can be placed in the operator

It establishes a multi-dimensional framework

- 1 Technical
- 2 Operational
- 3 Legal



Technical Criteria

- > **Documented risk assessment** covering the entire scope of the service.
- > **Annual updating** of information security and business continuity plans.
- > **Obligation to inform** the client in the event of a personal data breach.
- > **Appointment** of an information systems security manager.
- > **Appointment** of a physical security manager.
- > **Daily data backup** policy.



Operational Criteria

- > **Strong multi-factor authentication** to access administration interfaces.
- > **Nominative accounts** for users.
- > **An encryption mechanism** that prevents data recovery in the event of a resource or physical support reallocation.
- > **Segregation of network flows** (logical/physical/encrypted).
- > **Active monitoring** to manage technical vulnerabilities and evaluate risk exposure.



Legal Criteria

- > The provider's statutory headquarters, central administration, and principal establishment **must be established within an EU Member State.**
- > **Limits on the holding of capital and voting rights** by non-EU entities: 24% individually, 39% collectively.
- > **Storage and processing of data within the EU.**
- > **Justified compliance with GDPR principles** (legitimate purposes, limited data retention period).
- > The service agreement must include a **reversibility clause** providing for the secure restitution and erasure of the client's data upon contract termination or for any other cause.



The Qualification Procedure

- J0** Application for qualification submitted to ANSSI
- J1** Evaluation work accepted
- J2** Evaluation strategy accepted
- J3** Qualification decision by ANSSI.



- > Detailed description of the services submitted for qualification
- > Demonstration of conformity to the SecNumCloud framework
- > Selection of a qualified auditor responsible for conducting the J2 audits

- > Validation by ANSSI of the audit plan proposed by the evaluation body
- > Roadmap for J2 audits

- > Technical and organizational audits are conducted on-site by the accredited organization.
- > The report is transmitted to ANSSI for analysis.

- > ANSSI reviews the J2 audit report
- > Potential requests for corrective actions
- > Potential request for additional information or validation of the certification qualification

The Main Evaluation Criteria



Technical Criteria

- > Documented risk assessment covering the entire scope of the service.
- > Annual updating of information security and business continuity plans.
- > Obligation to inform the client in the event of a personal data breach.
- > Appointment of an information systems security manager.
- > Appointment of a physical security manager.
- > Daily data backup policy.



Operational Criteria

- > Strong multi-factor authentication to access administration interfaces.
- > Nominative accounts for users.
- > An encryption mechanism that prevents data recovery in the event of a resource or physical support reallocation.
- > Segregation of network flows (logical/physical/encrypted).
- > Active monitoring to manage technical vulnerabilities and evaluate risk exposure.



Legal Criteria

- > The provider's statutory headquarters, central administration, and principal establishment must be established within an EU Member State.
- > Limits on the holding of capital and voting rights by non-EU entities: 24% individually, 39% collectively.
- > Storage and processing of data within the EU.
- > Justified compliance with GDPR principles (legitimate purposes, limited data retention period).
- > The service agreement must include a reversibility clause providing for the secure restitution and erasure of the client's data upon contract termination or for any other cause.

SecNumCloud

Who is it?

Services Under Review for Qualification

	IN PROGRESS		QUALIFIED	
	Applicants	Offering	Provider	Offering
IaaS	Adista Bleu Cyllene ITS Ecritel Gip Mipih (Numih France) ITS Integra Numspot Orange Business OVH SAS Prolival - 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 is also undergoing qualification, but no public information is available on the type of qualification requested.

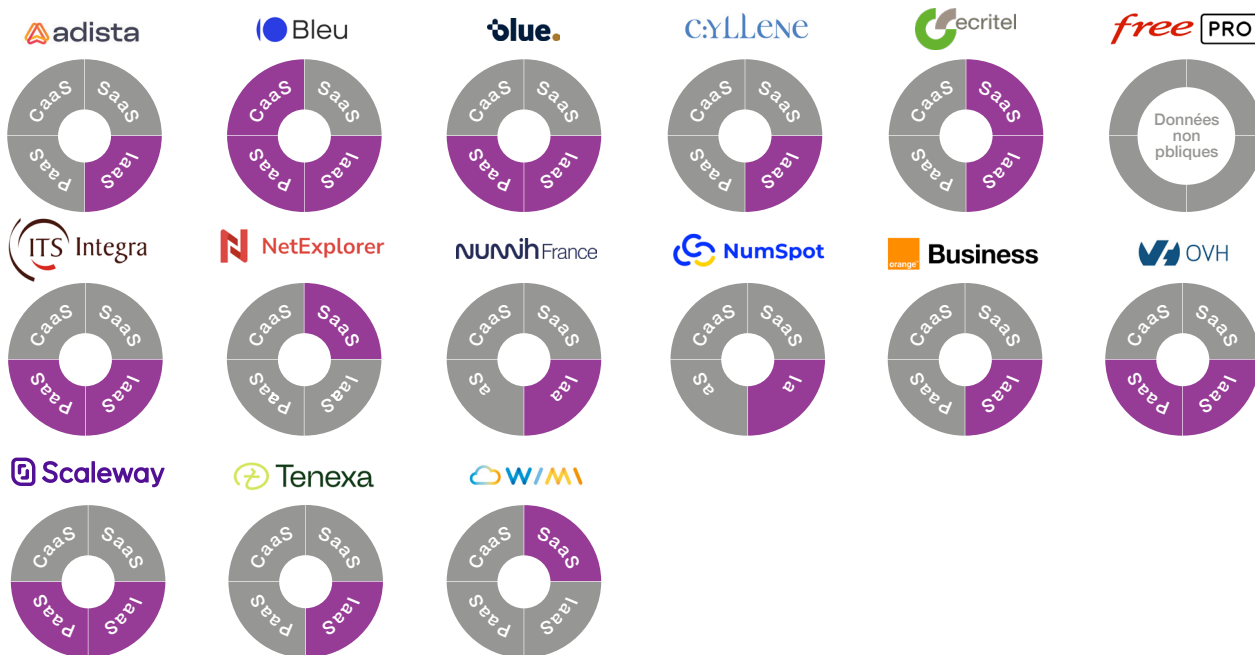
The candidates

IaaS	
Caas	
PaaS	
SaaS	

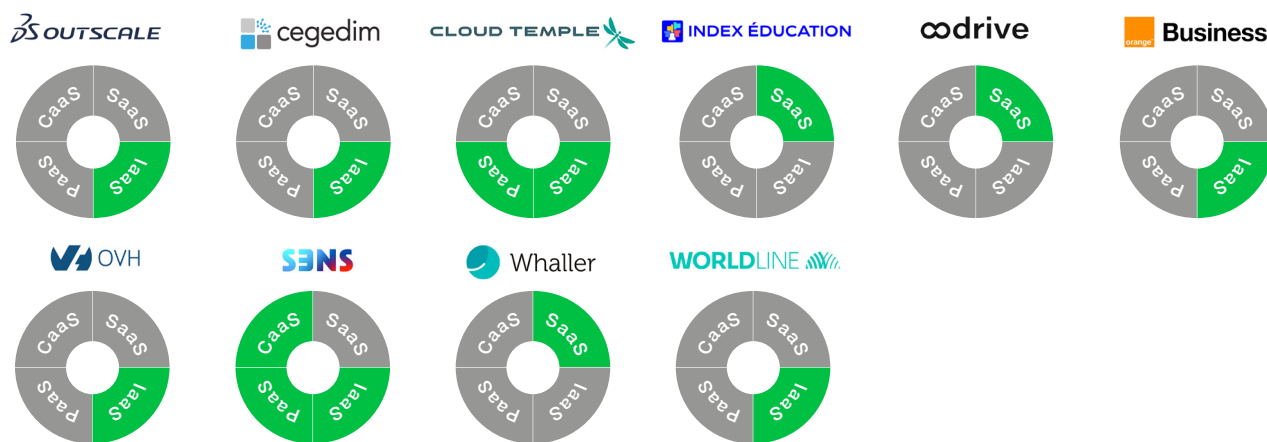


Scope of the qualification

IN PROGRESS



QUALIFIED PROVIDERS



Status of candidates

- J0** Application for qualification submitted to ANSSI
- J1** Evaluation work accepted
- J2** Evaluation strategy accepted
- J3** Qualification decision by ANSSI



Glossary of Cloud Offerings



IaaS (Infrastructure as a Service)

- > Provision of physical computing resources.
- > **The provider owns** the physical infrastructure and rents it or makes it available to a user.
- > **The client builds** his activity on this platform
- > **The provider** owns all the physical material, including machines, network, and storage.
- > **The client** builds the services according to his needs, decides the scope/perimeter, and determines the possible uses on the leased infrastructure.

The Specifics of IaaS

- **Strict segregation** between users.
- To prevent data recovery during resource reallocation or physical support recovery, **encryption (of the disk, file system, or by volume) with a key per client is required**

CaaS (Container as a Service)

- > Provision of tools allowing **the deployment, management, and orchestration of application** containers.
- > **A container** is like a small, isolated box that contains everything necessary for an application to function (libraries, code, tools, etc.), without interfering with others.
- > **The provider** manages the underlying infrastructure (servers, storage, network, operating system).
- > **The client** controls the containers and the technical elements related to their applications

The Specifics of CaaS

- **Strict segregation** between clients.
- **Recommended cryptography:** encryption by volume (one key/client).
- **Secure obliteration** at the end of the contract means the secure erasure of the encryption keys for the client's storage spaces.
- Administration and supervision operations must be carried out **from within the European Union**

PaaS (Platform as a Service)

- > Provision of a **technical platform ready for use** to develop, host, and run applications.
- > **The provider** manages the entire infrastructure part (network, servers, storage, operating system, etc.).
- > **The client** focuses on the development and management of their own applications

The Specifics of PaaS

- The provider has a **duty to inform** the client in case of modification to the software elements that the provider controls.
- **Strict segregation** between clients interfaces: the resources allocated for the use of one client must not be accessible to other clients

SaaS (Software as a Service)

- > Provision of **ready-to-use applications**, hosted in the cloud and fully managed by the provider.
- > The user simply accesses the application via the Internet—without having to install, host, or maintain anything.
- > **The provider** manages all the technical aspects requiring IT skills.
- > **The client** does not control the cloud platform but can modify configuration settings within the application.

The Specifics of SaaS

- **Multi-factor authentication** for end-user access.
- **Segregation** between the administration interfaces made available to clients and the interfaces allowing end-user access



of Cloud Temple

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

of SENS

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

of Bleu

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

of NumSpot

<https://numspot.com/en/produit/sovereign-data-aisovereign-data-ai/>

of Orange Business Services

<https://www.orange.com/en/press-release/orange-business-launches-new-trusted-genai-offers-end-to-end-for-french-customers-233858?>

of Scaleway

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

of Outscale

<https://en.outscale.com/cloud-experience/sovereign-cloud/>



MARCH 2026
EDITION