OBSERVATORY

SecNumCloud

JUNE 2026 EDITION

EDITORIAL SecNumCloud

Danish pragmatism and secure openness

Joen Magieres
Senior Policy Advisor, Danish Chamber of Commerce.

Europe's debate on digital sovereignty has intensified in recent years. Growing geopolitical tensions, cyber threats, concerns around critical infrastructure and strategic dependencies have pushed digital policy higher up the European agenda.

At the same time, European policymakers face a difficult balancing act: strengthening resilience and reducing strategic dependencies without further fragmenting Europe's already complex Digital Single Market.

From a Danish perspective, this balance is crucial. Danish policymakers and industry organisations increasingly view cybersecurity, resilience and supply-chain security as essential priorities. However, Danish companies find it difficult to thrive and scale-up on the European market and instead seek growth opportunities elsewhere.

In fact, eight out of twelve Danish unicorns have moved their headquarters abroad since the turn of the millennium, highlighting the challenge of scaling globally from within Europe.

When it comes to cloud trust, however, Denmark has taken a decentralized and risk-based approach centred around data protection, resilience and security. Rather than building a single sovereign cloud certification regime similar to SecNumCloud.

In practice, responsibility for cloud decisions largely remains with the individual organisation. Public authorities and private companies are expected to conduct their own risk assessments, procurement evaluations and compliance processes depending on the sensitivity of the data and services involved.

For personal data, the Danish Data Protection Agency provides guidance on lawful cloud use. On the cybersecurity side, NIS2 plays an increasingly important role. The Ministry of Resilience and Preparedness coordinates implementation, while 13 sectoral authorities supervise compliance. The Danish Agency for Digital Government is responsible for supervising cloud providers, data centres and certain digital infrastructure services under NIS2.

Unlike the French SecNumCloud-initiative, Denmark does not operate with any sort of formal exclusion of hyperscalers. Market access is generally open, and the debate is less about nationality as such and more about risk, resilience and dependency management. Decisions typically depend on factors such as the type of data involved, contractual safeguards, cybersecurity measures, GDPR compliance, supply-chain risks and procurement requirements.

Nonetheless, the momentum for Danish and European competitiveness is gaining traction – and for good reasons. Not just the often-mentioned reports from Draghi but also Letta and Niinistö have highlighted the writing on the wall. Neither the European market, competitiveness nor our resilience are in good shape. As such, European solutions are sought after even if it means a lower national focus. As our current Minister of Foreign Affairs puts it: We can't be a winner country in a loser region.

For that reason, the Danish Chamber has proposed a stronger and less fragmented Digital Single Market, greater harmonization of digital regulation, broader implementation of the 'Only Once' principle, and a more coordinated European approach to cybersecurity certification, digital infrastructure and resilience.

SecNumCloud

Cybersecurity and critical sectors at the Centre

Cybersecurity has become a progressively more essential element of the debate. Denmark is one of the world's most digitalised societies and therefore also one of the most digitally dependent and vulnerable. Both government and industry increasingly view cloud infrastructure as part of critical infrastructure.

This has become even more important following Russia's invasion of Ukraine, growing geopolitical tensions and a sharp increase in cyber threats targeting European countries. Danish policymakers and businesses are increasingly concerned about resilience, continuity of operations and dependencies in digital supply chains.

National security considerations become decisive in areas involving critical infrastructure, sensitive public-sector functions or security-classified information. In those cases, authorities and operators are expected to assess geopolitical exposure, supply-chain risks and operational dependencies carefully.

Denmark also has the D-Seal, a voluntary label for IT security and responsible data use. While it is not a sovereign cloud certification scheme or a mandatory market-access requirement, the Danish Chamber has argued that elements of the model could potentially inspire future European approaches to trusted digital infrastructure – e.g. on the back of a revision to the Cyber Security Act and the Cyber Security Certification Framework.

Hybrid versus sovereign digitalisation

The practical outcome is therefore not a strict sovereign-cloud model, but rather a hybrid and pragmatic approach. The Danish Chamber of Commerce has explicitly recommended a differentiated cloud strategy combining hyperscalers, hybrid cloud models, local providers and strategic partnerships.

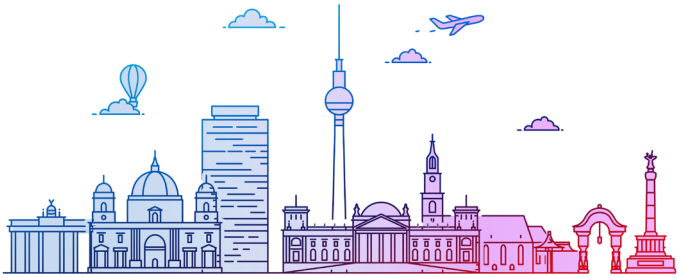
The Danish market nevertheless remains heavily dependent on non-European cloud providers. According to recent analysis from the Danish Chamber, 88% of member companies using cloud services rely on at least one non-European provider.

At the same time, 52% wish to reduce their dependency to some degree, primarily because of geopolitics, compliance concerns and supply-chain resilience.

Rather than pursuing strict digital sovereignty, Denmark's emerging approach could therefore best be described as "secure openness": maintaining access to global technologies while strengthening resilience, cybersecurity and strategic risk management around their use.

SecNumCloud
What's Up?

Hallo Deutschland!



THALES Google Cloud

Google Cloud and Thales have announced the creation in Germany of a twin entity to S3NS.

This new German sovereign cloud, operated by an entity controlled by Thales Germany, will comply with German sovereign cloud standards, notably the new C3A framework and C5 requirements. This announcement reflects the European reality of the sovereign cloud market. Private-sector players are operating at a European scale and are developing offerings that can be replicated beyond the borders of their initial domestic markets.

blue. | J1

Blue validates its J1 and progresses along the qualification path.

Scalingo

Scalingo enters the process with ANSSI to obtain the SecNumCloud qualification of its PaaS offering.

The project relies on the qualified SecNumCloud infrastructure of OUTSCALE, illustrating the progressive structuring of a sovereign PaaS ecosystem on top of already qualified IaaS layers.

C:YLLENE

Cyllène is no longer listed among the providers currently undergoing qualification by ANSSI.

Zoom of March Month : Sovereign Cloud at a European Scale

OVHcloud

Scaleway

S3NS

in alliance
with Post Telecom
and CleverCloud

in partnership
with Proximus, Clarence
and Mistral

The call for tenders covers the provision of cloud services for EU institutions, bodies and agencies, with a maximum value of €180 million over a six-year period. The selected providers were chosen based on their alignment with the European Commission's cloud sovereignty framework.

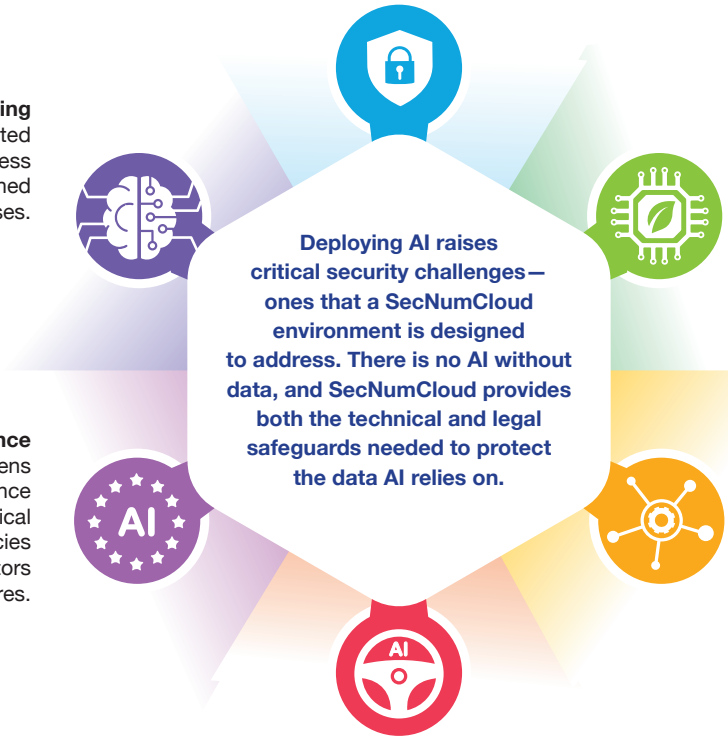
Zoom of February Month : Deploying AI in a SecNumCloud Environment

SecNumCloud: Secure, Scalable AI

Data protection & GDPR compliance
SecNumCloud reconciles AI innovation with stringent data-protection requirements, including for sensitive or critical information.

Model training
It enables better-calibrated AI, aligned with business needs and clearly defined use cases.

Resilience
SecNumCloud strengthens operational resilience by reducing critical dependencies on extra-European actors or infrastructures.



AI environmental impact
By hosting data centers in SecNumCloud environments, organizations benefit from France's energy mix and gain improved visibility into AI's environmental footprint.

End-to-end AI chain control
Deploying AI within SecNumCloud ensures consistent security, governance, and accountability across the entire AI value chain.

AI usage governance
Through access-control mechanisms and environment segmentation, organizations can establish clear, auditable AI governance. AI becomes a managed tool rather than a diffuse practice.

Integration Strategies

Offer 1

AI Infrastructure: GPU infrastructure within SecNumCloud — a technical offering designed to meet high-intensity AI computing needs.

Bleu
CLOUD TEMPLE
NumSpot
Business
Scaleway
S3NS

Offer 2

AI Platforms:
AI software deployed on SecNumCloud — with the cloud provider acting as an enabler.
> **LLM-as-a-Service operated by the cloud provider**
> **Client-operated solutions using dedicated AI software**

CLOUD TEMPLE
NumSpot
Business
OUTSCALE

Offer 3

AI Models:
The key is model-agnostic integration, ensuring flexibility in model selection and the ability to switch over time.

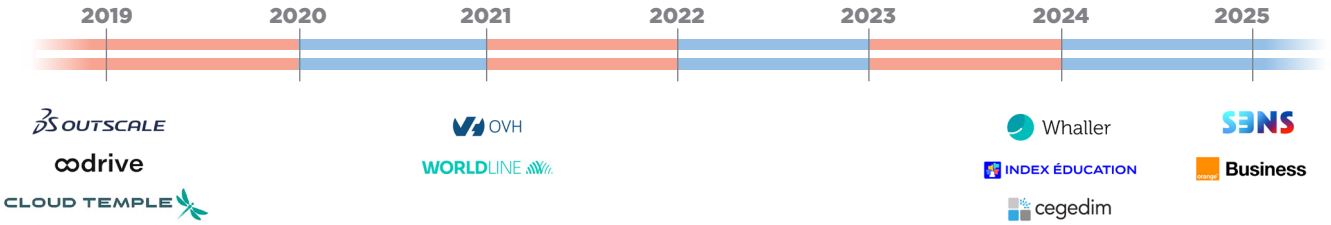
> **Open models: users retain control over model evolution**

> **Proprietary models: controlled by their owners and often more powerful**

Zoom of January Month : the Qualified Providers

Qualification: a Long-Term Corporate Commitment

Companies that have obtained SecNumCloud qualification were early movers in committing to the qualification process. Their decision reflects a near-civic form of engagement, demonstrating a strong alignment between corporate values and the security and trust objectives embedded in the SecNum-Cloud framework.



The Qualified Providers

	CLOUD TYPE	SHARE OF QUALIFIED OFFER	TARGETED CLIENTS	NUMBER OF MANAGED SERVICES	GEOGRAPHICAL PERSPECTIVE	QUALIFICATION BY COMPOSITION	PLANS TO EXTEND QUALIFICATION
OUTSCALE	Shared	30 50 80 100	Private Sector OIV/OSE Public Sector	10+	Europe	Facilitateur	✓
cegedim		Information not available					
CLOUD TEMPLE	Shared	30 50 80 100	Private Sector OIV/OSE Public Sector	20+	France	Facilitator	✓
INDEX ÉDUCATION		Information not available					
odrive		Information not available					
Business		Information not available					
OVH	Dedicated	30 50 80 100	SMEs Private Sector OIV/OSE Public Sector	20+	France	Facilitator	✓
S3NS	Shared	30 50 90 100	PME/TPE Secteur privé OIV/OSE Public Sector	50+	Europe	Facilitator	✓
WORLDLINE	Dedicated & Shared	30 50 80 100	Private Sector Public Sector	10+	France	Facilitator	✓
Whaller	Shared	30 50 80 100	SMEs Public Sector	10+	Monde	Beneficiaries	✓

Shared cloud: Hardware resources are shared across multiple tenants.
Dedicated cloud: Hardware resources are allocated exclusively to a single tenant.

Zoom of December Month : the PaaS

Scope of the PaaS and analysis criteria

PaaS is a strategic layer that enables the deployment of **managed services**, a key element in assessing provider maturity.

5 pillars to evaluate PaaS offerings

1 AI
Ability to develop/train/deploy AI models in a qualified SecNumCloud environment.
> *Stage 1 : GPUs*
> *Stage 2 : Native AI or LLM-as-a-Service*

2 MANAGED DATABASES
The capacity to host, operate, and secure a database engine without the client having to manage the servers or daily administration in a SecNumCloud qualified cloud environment.
> *Stage 1 : SQL*
> *Stage 2 : noSQL*

3 MANAGED ANALYTICS
The capacity to collect, store, process, and visualize data for analysis purposes, without client administration of the underlying infrastructure in a SecNumCloud qualified cloud environment.
> *Stage 1 : Visualization and simple queries*
> *Stage 2 : Big Data*

4 MANAGED STORAGE
The capacity to ensure the provisioning, availability, monitoring, and security of stored data, without client intervention on the infrastructure, all within a SecNumCloud qualified cloud environment
> *Stage 1 : Block Storage*
> *Stage 2 : File Storage*

5 INTEROPERABILITY WITH THIRD-PARTY EDITORS
The capacity of the platform to allow the deployment of services by independent software vendors in a SecNumCloud-qualified cloud environment.

A criterion for geographic availability also complements the analysis of these offerings.
The analysis of the offerings was carried out solely on publicly available information and based on the services submitted for qualification. In the future, actors can expand the scope of services submitted for SecNumCloud qualification.

The PaaS offering

	CLOUD TEMPLE	Bleu	Scaleway	S3NS
	Single cloud offering SecNumCloud qualified since 2022 Double qualification: IaaS and PaaS.	Offers Microsoft Azure and Microsoft 365 services in a SecNumCloud environment. Triple qualification in progress: IaaS, CaaS, PaaS.		Offers Google services in a SecNumCloud environment. Triple qualification in progress: IaaS, CaaS, PaaS.
Managed Analytics	STAGE 2	STAGE 2		STAGE 2
Managed Database	STAGE 2	STAGE 2		STAGE 2
Managed Storage	STAGE 2	STAGE 2		STAGE 2
AI platform	STAGE 2	STAGE 1		STAGE 1
Interoperability)				
Geography	FRANCE	FRANCE	EUROPE	EUROPE
	Qualified			

Unavailable
Available but not included in the SecNumCloud qualification scope
Available and included in the SecNumCloud qualification scope

OBSERVATORY

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.

J0

- 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

J1

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

J2

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

J3

- 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.

OBSERVATORY

SecNumCloud

Who is it?

Services Under Review for Qualification

IN PROGRESS

	Applicants	Offering
IaaS	**Adista**	dista Secure Cloud
	Bleu	Cloud de Confiance Bleu
	Cyllene ITS	IaaS SecNumCloud
	Ecritel	Ecritel Secure Cloud
	Gip Mipih (Numih France)	Cloud Premier Souverain
	ITS Integra	IT SecureCloud
	Numspot	Plateforme des services cloud
	Orange Business	Cloud Avenue SecNum Dynamic
	OVH SAS	SNC Cloud Platform
	Prolival - Groupe Tenexa	Horizon SecNumCloud
	Scaleway	Scaleway SecNumCloud
	Bretagne Télécom	Blue Secure Cloud
CaaS	**Bleu**	Cloud de Confiance Bleu
	ITS Integra	ITSecureKube
PaaS	**Bleu**	Cloud de Confiance Bleu
	OVH SAS	SNC Cloud Platform
	Scaleway	Scaleway SecNumCloud
SaaS	**Ecritel Solutions**	Ecritel Secure Backup
	NetExplorer	Share and Workspace
	Cloud Solutions	Wimi

QUALIFIED

	Provider	Offering
IaaS	**Cegedim**	CegNumCloud Secured IaaS
	Cloud Temple	IAAS Secure Temple
	OVH	Bare Metal Pod
	OVH	Hosted Private Cloud powered by VMware
	Orange Business	CloudAvenueSecNum
	Outscale	IaaS
	Worldline	Worldline Cloud Services
	S3NS	Cloud de Confiance PREMI3NS
CaaS	**S3NS**	Cloud de Confiance PREMI3NS
PaaS	**Cloud Temple**	PaaS Openshift
	S3NS	Cloud de Confiance PREMI3NS
SaaS	**Index Education**	EDT
	Index Education	Hyperplanning
	Index Education	Pronote
	Index Education	Pronote Primaire
	Oodrive	Oodrive_Work _Share
	Oodrive	Oodrive_Work
	Oodrive	Oodrive_Meet
	Whaller	Whaller Donjon SaaS

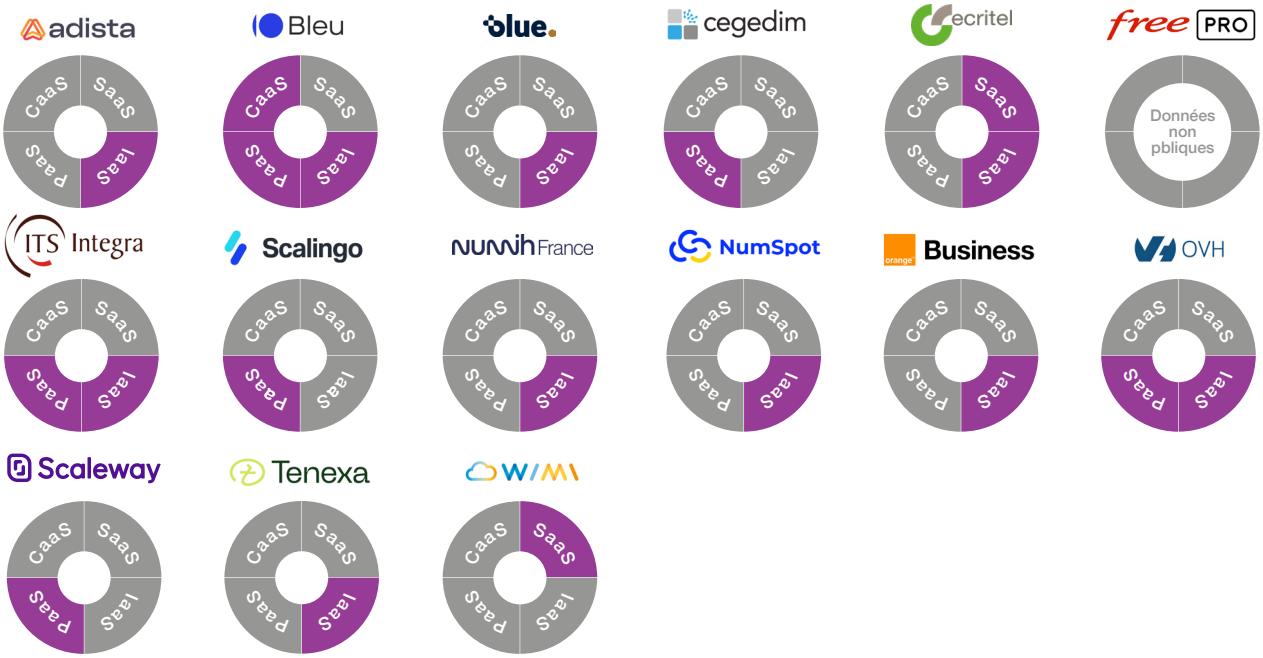
Free Pro is also undergoing qualification, but no public information is available on the type of qualification requested.

The candidates

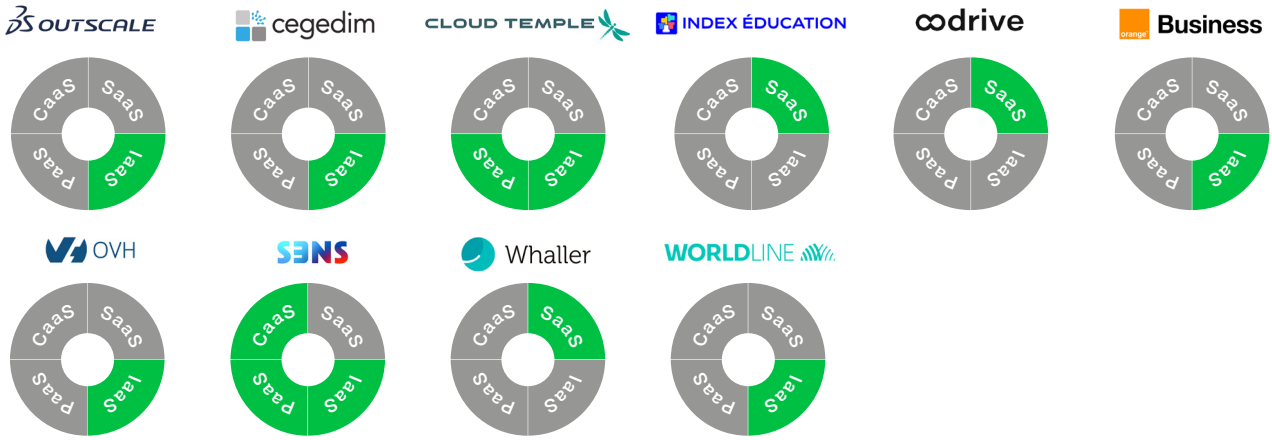
IaaS	adista, Bleu, Blue, Business, CYLLENE, ecritel, ITS Integra, NUMIH France, NumSpot, OVH, Scaleway, Tenexa
CaaS	Bleu, ITS Integra
PaaS	Bleu, OVH, Scaleway
SaaS	ecritel, NetExplorer, WIMI

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

J0

Tenexa
adista

J1

ITS Integra · Bleu · ecritel
blue. · NetExplorer
NumSpot · Scaleway

J2

J3

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 swithin 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*

JUNE 2026
EDITION