NISDUC #5 · CLOUD SOVEREIGNTY · BRUSSELS · 19 MAY 2026

SecNumCloud

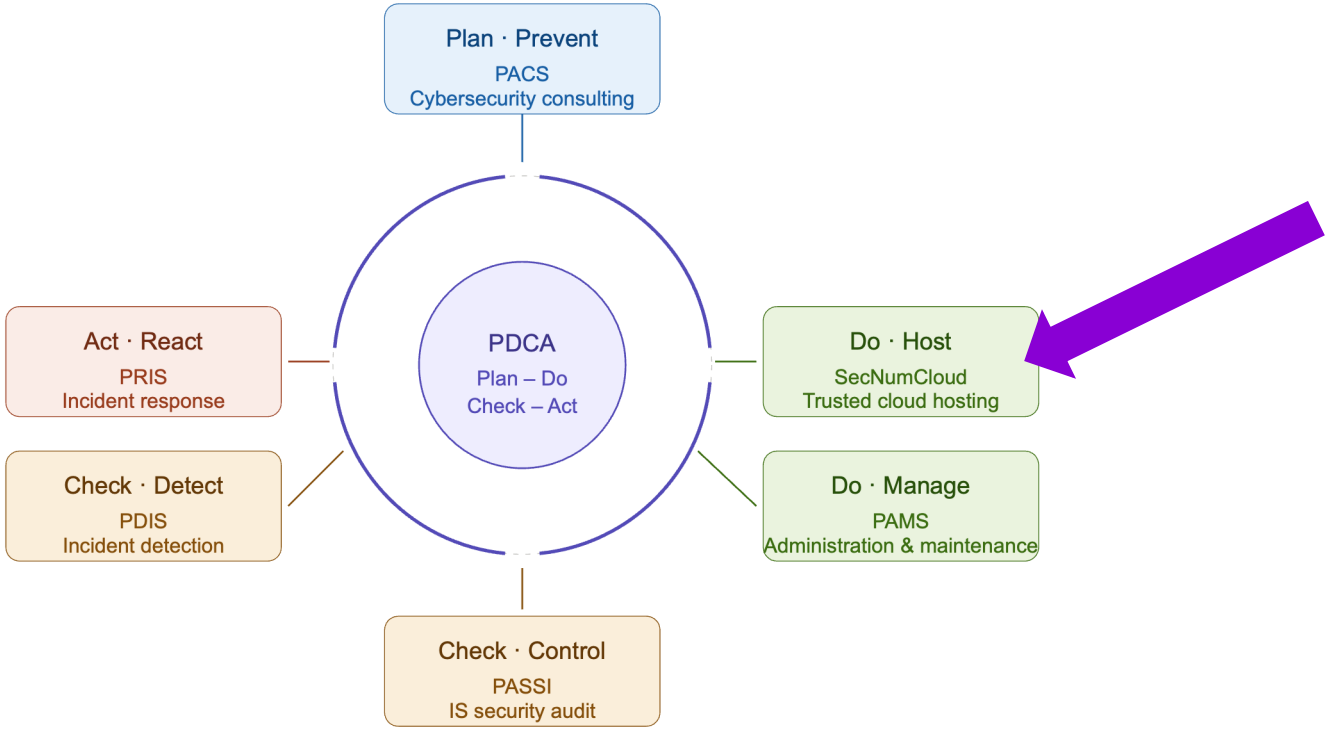
Qualification Experiences

A practitioner's view on France's cloud framework — and what it actually does (and doesn't) deliver.

Mouloud Ait-Kaci

CTO · Hackcyom · SecNumCloud evaluator & consultant

Intro to the merry world of ANSSI qualification schemes



We'll be here together for a quick 30min today ☺

ABOUT

Who's talking to you

Mouloud Ait-Kaci

CTO & founder of Hackcyom

- Graduate in pure maths and cryptology (IMAG, Université Grenoble Alpes 1)
- 13 years of experience in cybersecurity (CGI BC, Deloitte, S3, Hackcyom)
- PASSI qualified auditor (lead, pentest, configuration, architecture, source code, organizational)
- PACS qualified consultant (lead, homologation, risk management, secure architectures)
- SecNumCloud evaluator (lead, technical and organizational) since 2016
- SecNumCloud examiner by ANSSI delegation (wannabe SNC evaluator candidates' jury)
- PDIS evaluator (architecture and technical)
- PDIS examiner by ANSSI delegation
- ISO 27001 LI/LA certified, EBIOS RM certified
- Member of Club 27001 & Club EBIOS

Hackcyom

Boutique cyber firm · Paris · founded 2022

- HDS, ISO 27001, NIS2, SecNumCloud compliance & readiness consulting (ongoing PACS qualification)
- Audits: PASSI, all types
- Qualification evaluations and certification audits as a subcontractor for certification bodies (ISO27001, SNC, PDIS, eIDAS, etc.)
- Highly sensitive cloud building blocks provider :
  - Secure admin information system as a Service,
  - Class 1 Diffusion Restreinte information system as a Service over SNC
- Completely self-financed from scratch (no investors)
- **Disclaimer: vendor-neutral, no CSP affiliation**
- **Disclaimer^2: all said here is from publicly available information on the Web**

AGENDA

Where we're going

From concepts to a critical, practical toolkit.

01 — **Cloud sovereignty**

Setting the stage — and the vocabulary.

02 — **SecNumCloud**

What it actually is. And what it isn't.

03 — **Not all qualifications are equal**

A critical look at variations across offerings.

04 — **A user's guide**

How to choose a cloud provider — and own your risk.

05 — **Takeaways**

Lessons for European cyber teams, not just French ones.

01

SECTION ONE

Cloud Sovereignty: Setting the Stage

"Sovereignty" — a word that means too much

Six different things hide under the same flag.

Political

State autonomy from foreign powers.

Legal & jurisdictional

Whose law applies? Whose courts decide?

Data

Location, control, and access to data.

Operational

Who runs it, day to day, and from where.

Technological

Independence of stack: silicon, OS, software.

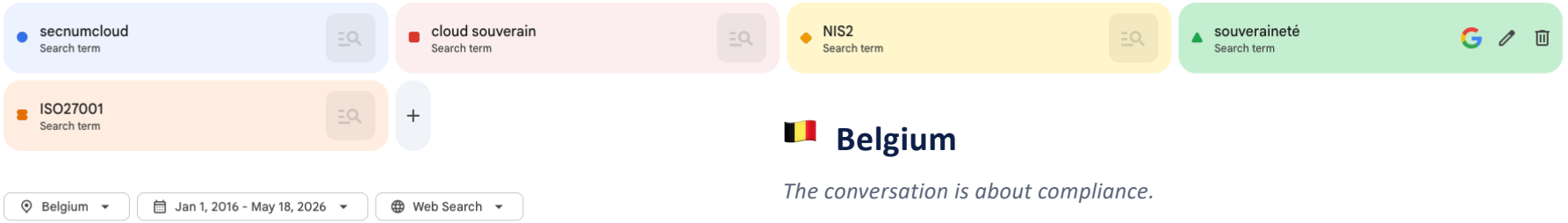
Strategic

Ability to act without external coercion.

So broad it risks meaning nothing — and that vagueness is now a marketing surface.

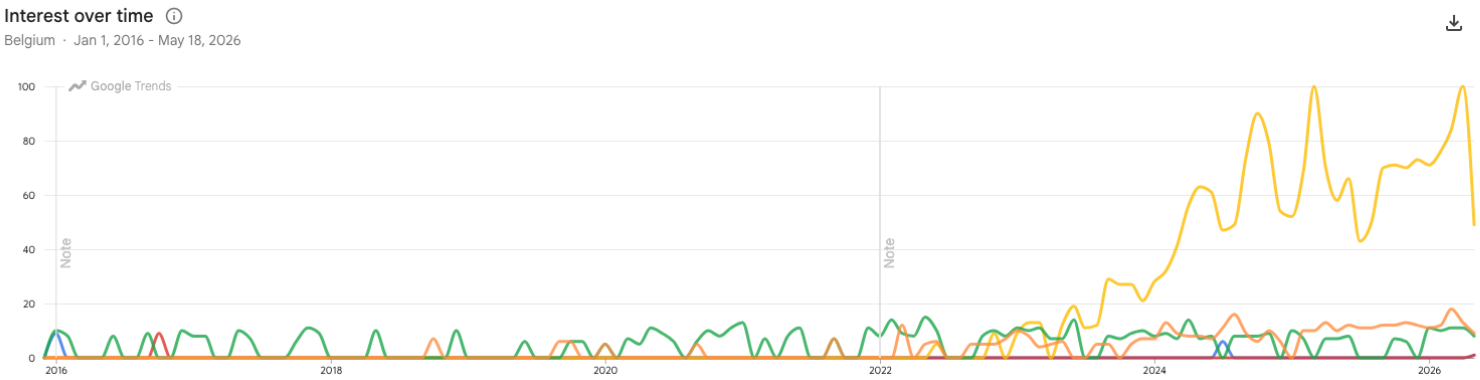
Same EU rules. Two very different conversations.

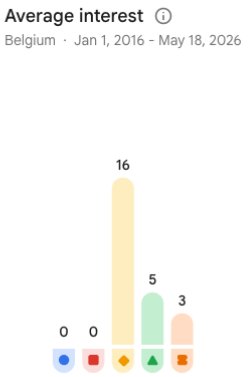
Average Google Trends interest, web search, Jan 2016 – May 2026.



Belgium

The conversation is about compliance.

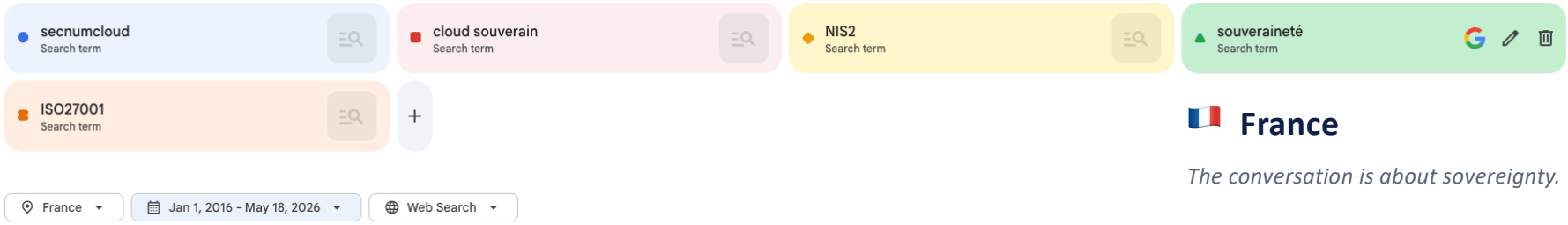




Source: Google Trends, web search, 2016–2026. Numbers = average relative interest.

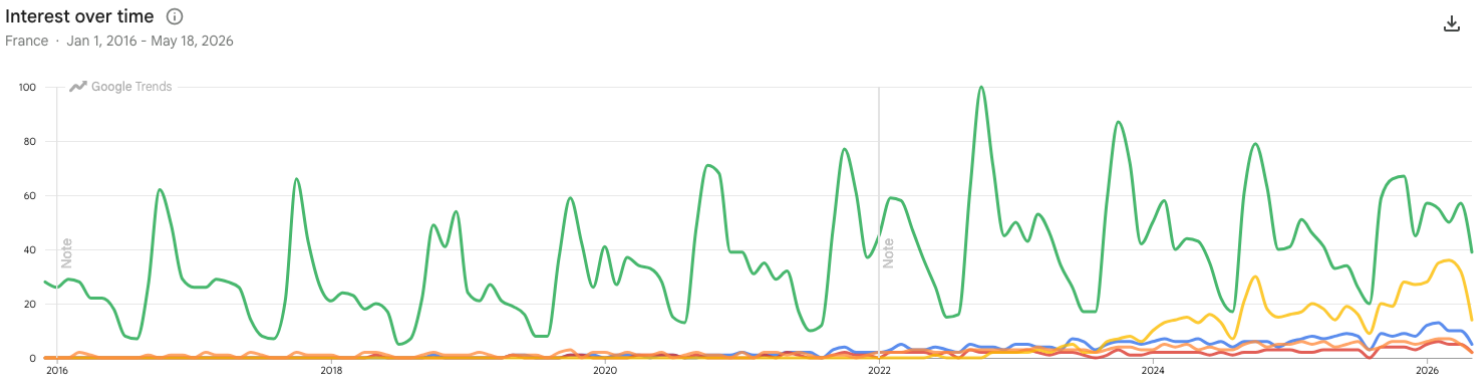
Same EU rules. Two very different conversations.

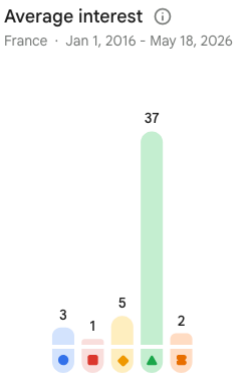
Average Google Trends interest, web search, Jan 2016 – May 2026.



France

The conversation is about sovereignty.





Source: Google Trends, web search, 2016–2026. Numbers = average relative interest.

Sovereignty ≠ Technological independence

Conflating the two is the #1 reason "sovereign cloud" debates go nowhere.

SOVEREIGNTY

Who can compel access?

A legal & political question.

- Whose courts have jurisdiction?
- Which extraterritorial laws apply?
- Who governs the operator?
- Who owns the shares & decisions?

TECHNOLOGICAL INDEPENDENCE

Can you run it without them?

An engineering & supply-chain question.

- Whose silicon, OS, hypervisor?
- Whose software licences?
- Whose updates and support?
- Could you keep operating if cut off?

A "sovereign" cloud can still run on foreign silicon. An "independent" stack can still sit under foreign law. Don't confuse them.

Three concrete reasons we have this debate

Beyond ideology, the threat model is documented.

01

LEGAL EXTRATERRITORIALITY

Foreign law reaching into your data

US CLOUD Act (2018), FISA §702, Executive Order 12333. A US-owned provider can be compelled to hand over data, regardless of where it sits — and is generally barred from telling the customer.

02

ECONOMIC INTERFERENCE

Industrial espionage is not theoretical

The Frédéric Pierrucci case (Alstom, 2013–14) is the textbook reminder that extraterritorial law has been instrumentalised against European industrial competitors. A reading list, not a conspiracy.

03

SERVICE SUSPENSION

The cloud kill-switch risk

May 2025: the ICC's Chief Prosecutor reportedly lost access to Microsoft email services amid US sanctions. Availability is a sovereignty question now, not just a contractual SLA.

None of this requires anyone to be "hostile". It just requires the law of another state to apply.

02

SECTION TWO

SecNumCloud: What It Is (and Isn't)

SecNumCloud at a glance

A French national qualification — six facts before the debate.

ISSUED BY

ANSSI

France's national cybersecurity agency

CURRENT VERSION

3.2

Published 2022 — basis of the EU "High+" debate

NATURE

Qualification

Not a certification — ANSSI decides

REQUIREMENTS

~390 requirements

Over 1200 Technical + organizational controls

PROCESS

4 milestones

Gated process, ~18–36 months in practice

QUALIFIED OFFERS

~20

IaaS, PaaS, CaaS, increasingly SaaS (but very hard to achieve)

What SecNumCloud IS

A serious cybersecurity baseline. Don't underestimate it.

A technical cybersecurity baseline

Strong, prescriptive requirements on isolation, encryption, identity, admin operations, supply chain, business continuity, audit.

A product-level qualification (ISO 17065)

Unlike ISO 27001 (management system, ISO 17021), SecNumCloud certifies the service itself. Different audit posture entirely.

A guided, gated process

Four milestones reviewed by ANSSI. Skilled evaluators work to a guide validated by ANSSI. Heavy on evidence — not box-ticking.

A transparency mechanism

Clause 19.6 documents (and constrains) exposure to non-European extraterritorial law. It doesn't eliminate it — it makes it visible.

A reference for sensitive French public-sector data

Currently the only EU national scheme used as a procurement gate for sensitive public data. EUCS is following — see section 03.

What SecNumCloud is NOT

Five honest disclaimers about a useful framework.

A sovereignty label

The word "sovereignty" doesn't appear in the spec. It addresses cybersecurity, with one clause on extraterritorial-law transparency. That's not the same thing.

A guarantee of technological independence

Composition with non-EU technology is allowed — under strict operational and isolation conditions. See: S3NS, the most-discussed example.

Equivalent to ISO 27001

27001 audits how you manage risk. SecNumCloud audits whether the service meets ~390 specific controls. Largely complementary, not interchangeable.

One-size-fits-all across IaaS / PaaS / SaaS

Same referential, very different shapes of audit. Composition (a PaaS on a qualified IaaS) introduces real complexity.

A replacement for your risk management

The qualification certifies the provider's posture. Your risks, your data, your accountability — those don't move.

Case study: S3NS · qualified December 2025

The most instructive recent example — and the most contested.

THE FACTS

A Thales × Google joint venture, SecNumCloud-qualified.

- Founded 2022. French company, 100% controlled by Thales.
- Offering: PREMI3NS — built on Google Cloud technology.
- Qualified by ANSSI on 17 Dec 2025, SecNumCloud 3.2.
- First-ever simultaneous IaaS + CaaS + PaaS qualification.
- Operated exclusively by S3NS staff, in French data centers.
- Every Google update intercepted in a quarantine zone first.

WHAT IT TELLS US

The framework explicitly allows hybrid stacks.

- Tech provenance is one input, not the verdict.
- What matters: operational control, jurisdiction, isolation.
- S3NS satisfies ANSSI's clause 19.6 — the framework's only sovereignty-adjacent requirement.
- It still raises real questions on tech dependency, exit, and SEAL scoring (next section).

S3NS isn't an exception.
It's the model the framework was designed to permit.

03

SECTION THREE

Not All SecNumCloud Are Equal

Same label. Six dimensions of real variation.

Two SecNumCloud offers can be qualitatively very different.

01

Isolation

Physical isolation vs logical / cryptographic. Same word, very different architectures.

02

Encryption

Customer-held keys (BYOK/HYOK) vs CSP-held keys. Who really controls cleartext access?

03

Composition

Pure proprietary stack vs reliance on third-party (qualified) IaaS or PaaS.

04

Ownership

100% EU capital and control vs hybrid JVs. Corporate governance matters.

05

Operations

Where do the admins sit? Which laws apply to them and to their employer?

06

Scope of qualification

Which exact services are in scope? Where does the qualified perimeter stop?

Enter the EU Cloud Sovereignty Framework

Published by the European Commission on 20 October 2025 — finally puts numbers on the debate.

8	0→4	20%	v1.2.1
Sovereignty Objectives (SOVs)	SEAL assurance levels	Highest-weighted SOV: supply chain	Current version (Oct. 2025)

The SEAL ladder — from no sovereignty to full sovereignty.

SEAL-0
No Sovereignty
Fully under non-EU control & law.

SEAL-1
Jurisdictional
EU law applies on paper. Foreign parent can compel access.

SEAL-2
Data Sovereignty
EU law applicable AND enforceable. Minimum threshold for EU tenders.

SEAL-3
Digital Resilience
Immune from non-EU supply-chain disruption.

SEAL-4
Full Sovereignty
Complete EU control, silicon to application.

Source: European Commission DG DIGIT, Cloud Sovereignty Framework v1.2.1, October 2025.

SecNumCloud providers — mapped against sovereignty objectives

Estimated SEAL scores per SOV, based on public information. (Non official) Scores reflect best available offering per provider based on public information.

		EU Cloud Sovereignty Framework — 8 Objectives								
Provider	Type	SOV-1 Strat. 15%	SOV-2 Legal 10%	SOV-3 Data 10%	SOV-4 Ops 15%	SOV-5 Supply 20%	SOV-6 Tech 15%	SOV-7 Sec. 10%	SOV-8 Env. 5%	SEAL est.
3DS Outscale	IaaS	4	4	4	4	4	4	4	3	3–4
Cloud Temple (OpenIaaS)	IaaS+	4	4	4	4	4	4	4	3	3–4
Oodrive	SaaS	4	4	4	4	4	4	3	3	3–4
Index Education	SaaS	4	4	4	4	4	4	3	3	3–4
Whaller	SaaS	4	4	4	4	4	4	3	3	3–4
OVHcloud	IaaS	4	4	4	4	3	3	4	4	3
Orange Business	IaaS	4	4	4	4	3	2	4	4	3
Worldline	IaaS	4	4	3	4	3	2	3	3	3
Cegedim	IaaS	4	4	3	4	3	2	4	3	3
S3NS (Thales×Google)	IaaS+	3	3	3	4	1	1	4	3	2

Key pattern: SOV-5 (supply chain, 20%) and SOV-6 (technology, 15%) are where providers diverge most. The VMware/Broadcom dependency caps most IaaS providers at SEAL-3.
Only Outscale (TINA OS) and Cloud Temple OpenIaaS (Vates/XCP-ng) achieve 4/4 on both — on a fully EU, open-source hypervisor.

Same provider. Same label. Different sovereignty.

Cloud Temple holds two qualified IaaS offerings — one scores SEAL-2, the other SEAL-3/4. Both are SecNumCloud 3.2.

VMWARE IAAS

Secure Temple (IaaS)

VMware vSphere · Broadcom (US) · proprietary licence

SOV-1 Strategic	4/4
SOV-2 Legal	4/4
SOV-3 Data	3/4
SOV-4 Ops	4/4
SOV-5 Supply chain	2/4
SOV-6 Technology	2/4
SOV-7 Security	4/4
SOV-8 Environment	3/4

SEAL-2 estimated

Capped by Broadcom dependency

VS

OPEN IAAS (VATES / XCP-NG)

OpenIaaS (IaaS)

XCP-ng · Vates (FR) · open-source · auditable

SOV-1 Strategic	4/4
SOV-2 Legal	4/4
SOV-3 Data	4/4
SOV-4 Ops	4/4
SOV-5 Supply chain	4/4
SOV-6 Technology	4/4
SOV-7 Security	4/4
SOV-8 Environment	3/4

SEAL-3/4 estimated

EU open-source stack unlocks it

Both carry the SecNumCloud 3.2 label. ***Only one achieves sovereignty at the supply-chain and technology levels.*** ***The label doesn't tell you which.***

April 2026: the EU's first sovereign cloud tender

€180M, 6 years, 4 awardees, scored against SEAL — and the results tell a story.

AWARDEE	COMPOSITION	SEAL	NOTE
Post Telecom (LU) + OVHcloud + Clever Cloud	Own EU technology	**SEAL-3**	*Digital resilience*
StackIT (DE)	Own EU technology	**SEAL-3**	*Digital resilience*
Scaleway (FR)	Own EU technology	**SEAL-3**	*Digital resilience*
Proximus (BE) + S3NS, Clarence, Mistral	Includes Google-based S3NS	**SEAL-2**	*Minimum threshold*

Same SecNumCloud label — different EU sovereignty scores.

S3NS is SecNumCloud-qualified — yet pulls the Proximus consortium to SEAL-2 because of Google-origin technology. No awardee reached SEAL-4.

04

SECTION FOUR

A User's Guide

The label transfers transparency. Not accountability.

A reminder that NIS2 makes more uncomfortable than it used to be.

THE PROVIDER

Provides the platform

- Operates the qualified service
- Holds the technical baseline
- Documents the perimeter & limits
- Audited every cycle

THE CUSTOMER

Owns the risk

- Remains the data controller
- Decides what workloads to entrust
- Owns the consequences of incidents
- Owns the exit strategy

THE NIS2 ANGLE

Makes it personal

- Executive accountability (Art. 20)
- Reporting obligations stay with the entity
- A SecNumCloud CSP is supply chain, not absolution
- Document your sovereignty rationale

Outsourcing the platform is fine. Outsourcing the responsibility isn't possible.

Eight questions worth asking — even of a qualified CSP

These are not adversarial. They simply make the label legible.

01 What's actually in scope of the qualification — which exact services?

02 Is there composition? Which sub-services rely on another (qualified) provider?

03 Where do the admins sit, and which laws apply to them and their employer?

04 Who owns the shares? Any non-EU influence on governance or strategic decisions?

05 What's the provenance of the underlying technology? Hypervisor, storage, network?

06 How are encryption keys managed? Customer-held? Customer-controlled? Or CSP-held?

07 What happens if an upstream non-EU dependency cuts you off? Documented exit plan?

08 When was the last surveillance audit, and what was the latest ANSSI signal?

How to actually use SecNumCloud — without overclaiming it

Treat it as a powerful input, not the verdict.

DO

- ✓ Use it as a starting baseline, not the finish line.
- ✓ Cross-reference SecNumCloud against the EU SEAL framework.
- ✓ Combine with: BYOK/HYOK, BCP/DR, contractual safeguards, exit plans.
- ✓ Map qualified services against your sensitive workloads, not your whole IS.
- ✓ Document your sovereignty rationale for NIS2 management body.

DON'T

- ✗ Don't treat "Sovereignty" as a binary yes/no thing.
- ✗ Don't assume composition is transparent without asking.
- ✗ Don't equate SecNumCloud with sovereignty in board-level reporting.
- ✗ Don't outsource your due diligence to the label.
- ✗ Don't ignore the SEAL score now that there is a quantified yardstick.

05

SECTION FIVE

Takeaways

Five lessons, applicable beyond France

Things that hold for any EU sovereignty-adjacent framework.

01

Sovereignty is a spectrum, not a binary.

The SEAL ladder (0–4) makes this measurable. Most real options sit at SEAL-2 or SEAL-3 today.

02

Cybersecurity frameworks ≠ sovereignty labels.

SecNumCloud secures. It doesn't make sovereign. The same lesson applies to EUCS, CyFun, BSI C5, ENS.

03

Composition is the elephant in the room.

Hybrid stacks (EU operations on non-EU tech) are now explicitly permitted. Make the case-by-case judgment.

04

The customer always owns the residual risk.

Under NIS2, executive accountability is personal. A label transfers transparency — never accountability.

05

Align deliberately — before the regulator does it for you.

EUCS revision, the EU Cloud Sovereignty Framework, the upcoming Cloud & AI Development Act: the picture is consolidating fast.

“

Don't read the sticker.

Read the small print.

Frameworks help. They never decide for you.

Thank you

Questions, push-back, war stories — all welcome.

Mouloud Ait-Kaci

CTO & founder · Hackcyom

WEB contact@hackcyom.com

LINKEDIN linkedin.com/in/makcyom