

SOVEREIGN, OR PAINTED ON?

Grading a sovereignty claim at the resolution that matters — the sovereignty spectrum, applied.

June 2026



We create intelligent customers.



TABLE OF CONTENTS

Key Judgements:.....3

The Sovereignty Spectrum:.....4

 Non-sovereign.....4

 Partially Sovereign.....4

 Majority Sovereign.....4

 Sovereign.....5

Where The Spectrum Sits In A Decision:.....6

The Spectrum Applied – A Worked Example:.....7

 Compute And Storage.....7

 Control Plane (Determinant).....7

 Key Custody (Determinant).....7

 Identity Plane (Determinant).....7

 The AI Model (Determinant).....7

What A Competent Buyer Does:.....9

Conclusion:.....10

Author:.....11

Sources:.....12

KEY JUDGEMENTS:

1. “Sovereign” is assessed today at the wrong resolution — the operator, the data centre, the contract. At that resolution almost any offering can be made to pass. Graded at the level of components and their composition, the same offering routinely lands one or two bands lower. (High confidence. This follows directly from the Strategic Architecture Framework, and is consistent with the public record.)
2. Sovereignty is not a yes or a no. It is a degree, held across four bands — Non-Sovereign, Partially Sovereign, Majority Sovereign, Sovereign. Collapsing that gradation into a single tick is precisely what allows a painted-on claim to survive a procurement. (High confidence.)
3. The band a system occupies is set by who can lawfully reach the components that determine control — not by where the data is stored. Those determinant components are the control plane, the keys, the identity plane, and any model whose behaviour its provider can change. A domestic address moves none of them. (High confidence.)
4. A “sovereign cloud” sold on a domestic region and a domestic contract, while its control plane, key custody, or model updates remain under foreign operating control, is Partially Sovereign at best. The gap between the claim and the band is invisible to a contract-level assessment, and it is the most common composite we see. (Medium-to-high confidence.)
5. The remedy is not more assurance against the wrong question. It is to grade the claim at component resolution before signature — and to have one voice in the room with no reason to grade it generously. For sensitive workloads this has stopped being good procurement practice and become a security control. (This is the paper’s central claim. It is argued below, not asserted here.)





THE SOVEREIGNTY SPECTRUM:

Sovereignty, properly understood, is a legal posture: which authorities have lawful reach into which parts of a system, on what grounds. The Strategic Architecture Framework makes the point that this posture is almost always assessed at too coarse a grain to be useful — at the level of the operator, the data centre, or the contract — when the property that matters lives at the level of the components and their composition.[1]

The sovereignty spectrum is that assessment carried out at the right grain: sovereignty graded, component by component and then as a whole, rather than collapsed into a single claim. It is the instrument that sits beneath the harder operational question the framework calls contestability — whether you could keep operating if the reach were exercised against you.

Not every component carries equal weight, and grading the whole by averaging across every box on a diagram flatters the result. The bands are set by the determinant components — the small set whose compulsion or withdrawal changes whether the operator still holds control:

- ▶ the control plane — where administration actually happens, and under whose hand;
- ▶ key custody — who can produce the keys under lawful compulsion, regardless of who is nominally “customer-managed”;
- ▶ the identity plane — whose directory decides who is authenticated, and from where;
- ▶ the model — whose weights, updated by whom, with inference running where;

and, for each of the above, the operating and parent jurisdiction, and any extraterritorial reach.

NON-SOVEREIGN

The determinant components are operated, owned, and key-held abroad. The domestic party holds use, not control. Foreign reach is routine, not exceptional.

PARTIALLY SOVEREIGN

Hosting and contract are domestic, but one or more determinant components remain under foreign operating control, foreign key custody, or foreign update. This is where the “sovereign cloud with a flag painted on” sits.

MAJORITY SOVEREIGN

The determinant components are domestically operated and controlled. Residual foreign reach is confined to non-determinant components, or to mechanisms the operator can sever without losing the capability.

SOVEREIGN

Every determinant component is operated, owned, and key-held within the jurisdiction. Where foreign reach exists at all, it cannot alter, observe, or withdraw the capability.



The grading is produced by a short, fixed set of questions, asked of each determinant component and then composed. None requires clearance, secret knowledge, or a six-month engagement:

- ▶ Which legal entity operates it, and where is that entity incorporated?
- ▶ Who controls that entity, and under whose law?
- ▶ What law, treaty, or order reaches it regardless of the contract?
- ▶ Where is the control plane operated, and by whom?
- ▶ Who can produce the keys under lawful compulsion?
- ▶ Whose model weights, updated by whom, with inference running where?
- ▶ Can the operator remove the component without losing the capability?

A claim that cannot survive these questions at component resolution was never sovereign in the property that mattered. It was sovereign in the property that happened to be measured.



We create intelligent customers.



WHERE THE SPECTRUM SITS IN A DECISION:

The band is never read in a vacuum. It is read against the sensitivity of the data and the assurance the sensitivity demands. For UK work that means the classification tiers from OFFICIAL to TOP SECRET and their respective regimes — Cyber Essentials, Gov Assure, and the JSP, NIST, and NATO assurance directives — with particular attention to the point at which aggregated non-sensitive data quietly becomes sensitive.[2][3]

Two continuous activities feed the grading. *Continuous analysis* vets the people and the provenance behind a component — the nation and its trade relations, the owner, the actor — and produces the risk picture. *Continuous assurance* vets the artefacts themselves — the hardware, the software, the services. The risk is expressed not as an adjective but on the PHIA probability yardstick, so that “unlikely” and “likely” carry the same meaning for the engineer and for the minister.[4]

The spectrum is where the two meet: the band a component can hold for a given classification, and the composition that results when the components are placed together. The fuller decision model — tiers, regimes, vetting, and the supply-chain and resilience co-dependencies that link them — is the working view for the architect. The spectrum is the part the person who signs needs to be able to read.

THE SPECTRUM APPLIED – A WORKED EXAMPLE:

What follows is a composite, drawn from recurring practice. It names no provider and no programme; every step is one we have seen made, and defended, in good faith. A public-sector buyer is offered a “sovereign, secure” cloud for OFFICIAL-SENSITIVE workloads — data that is persistent and, once aggregated, sensitive.

The claim rests on three facts, each of them true: the service runs in a domestic region; the operating entity is a domestically incorporated subsidiary; the contract is under domestic law. At contract resolution the system reads as sovereign. The spectrum asks the same question of the components that actually decide the matter.

COMPUTE AND STORAGE

Operated by the domestic subsidiary; owned by a foreign parent; reachable by the parent’s jurisdiction through extraterritorial legislation regardless of the domestic contract.[5] Operating jurisdiction home; control foreign-owned and foreign-reachable.

CONTROL PLANE (DETERMINANT)

Administration is performed through a control plane operated centrally, outside the domestic region. The domestic operator administers by permission, not by control.

KEY CUSTODY (DETERMINANT)

The encryption is real and the keys are described as “customer-managed.” The customer’s keys are wrapped by a provider root and recoverable through a provider process that the parent jurisdiction can compel.[6] Effective key control sits abroad.

IDENTITY PLANE (DETERMINANT)

Authentication is federated to a provider-operated directory whose decisions depend on the same out-of-region control plane. Who is admitted, and who is locked out, is decided elsewhere.

THE AI MODEL (DETERMINANT)

The “AI-enabled” headline is a foundation model reached through the provider’s managed service. Its weights and its update schedule are controlled by a third party in another jurisdiction, and the deployable variant is smaller than the flagship the brand name evoked. Provenance and the power to change its behaviour both sit abroad.



We create intelligent customers.



Four of the five determinant components are under foreign operating control, foreign key custody, or foreign update and compulsion. The hosting region and the contract — the facts the claim was built on — are not determinant. The composition lands the system in Partially Sovereign, toward its lower edge. The distance between the “Sovereign” on the cover sheet and the Partially Sovereign on the spectrum is the painted-on gap, and it is precisely the distance a contract-level assessment cannot see.

None of this requires anyone to have behaved badly. Each component is defensible on its own. The exposure is a property of the composition — and the composition is the one thing no party at the table was paid to grade.

WHAT A COMPETENT BUYER DOES:

The instrument is only useful if it changes what happens before signature. For a senior buyer it reduces to a short discipline that can be applied without anyone's permission:

- ▶ Specify the band, not the adjective. State the minimum band the classification requires, and require it of the determinant components specifically — not of the system “overall.”
- ▶ Require the grading as a deliverable you keep. The component-resolution assessment is an artefact the buyer holds and can act on without the supplier in the room. If the supplier will not produce it, that refusal is itself the finding.
- ▶ Ask the seven questions before signature, of each determinant component. A claim that cannot answer them was never a product; it is a build you are funding, or a dependency you are renting.
- ▶ Treat any determinant component under foreign operating control as disqualifying for the tier — unless it can be severed without losing the capability. Severability is the test that separates Majority Sovereign from Partially Sovereign.

The cost of grading the claim at this resolution is a few days. The cost of discovering the band after signature is the programme.



We create intelligent customers.



CONCLUSION:

The sovereignty spectrum does nothing clever. It grades a claim at the resolution the claim was built to survive, names the components that actually decide the matter, and puts the result on a scale a minister and an engineer can read together. The painted-on cloud is not defeated by suspicion, or by more assurance against the wrong threat. It is defeated by being graded honestly, once, before the money moves — by someone in the room with no reason to grade it kindly. The result is the only thing any of this was ever for: better decisions, and less risk.

AUTHOR:

James Patrick, CITP MBCS

Founder of Nuraghe. Chartered IT Professional, TechUK National Security Committee, former intelligence officer, peer-reviewed NATO author. He assures secure systems for the most demanding classified environments in allied and UK governments, and authored AI 101, now taught across defence from Major to four-star General.



We create intelligent customers.



SOURCES:

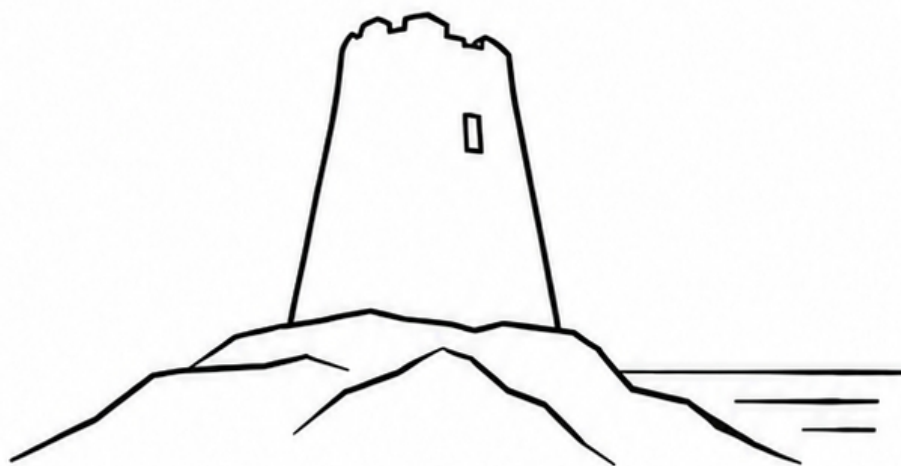
1. Patrick, J. (2026). The Strategic Architecture Framework: the layer above enterprise architecture which underpins security (First Edition). Licensed CC BY 4.0. Establishes contestability as a distinct architectural property and the case for assessing sovereignty at the level of components and their composition rather than the operator, data centre, or contract.
2. Cabinet Office, Government Security Classifications Policy. Defines the OFFICIAL, SECRET, and TOP SECRET tiers and the handling each requires, including the treatment of aggregation.
3. National Cyber Security Centre / GOV.UK, Secure by Design; and the assurance regimes referenced in practice — Cyber Essentials, Gov Assure, and the relevant JSP, NIST (SP 800-37/800-53), and NATO assurance directives.
4. Professional Head of Intelligence Assessment (PHIA), probability yardstick. The calibrated scale used here to express likelihood, so that the same word means the same thing to the engineer and to the decision-maker.
5. US Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018. Establishes lawful reach over data held by providers subject to US jurisdiction, regardless of where the data is physically stored — the mechanism behind foreign parent- jurisdiction reach into a domestically hosted service.
6. European Union, Data Act (Regulation (EU) 2023/2854), Chapter VII; and GDPR (Regulation (EU) 2016/679), Article 48. The instruments behind the principle that a European — or any domestic — data-centre address changes the geography but not the jurisdiction: control follows the provider, not the building. Corroborated on oath before the French Senate's commission d'enquête on digital sovereignty (June 2025), where a major provider confirmed it could not guarantee domestically held public-sector data against access under its home jurisdiction's law.

Sources are cited to verifiable public record. Where this paper describes recurring patterns from practice, it does so in general terms and names no specific programme, supplier, or client.

NURAGHE

(nʊˈrɑːɡeɪ)

Sovereign technology strategists
for government and defence.



We create intelligent customers.