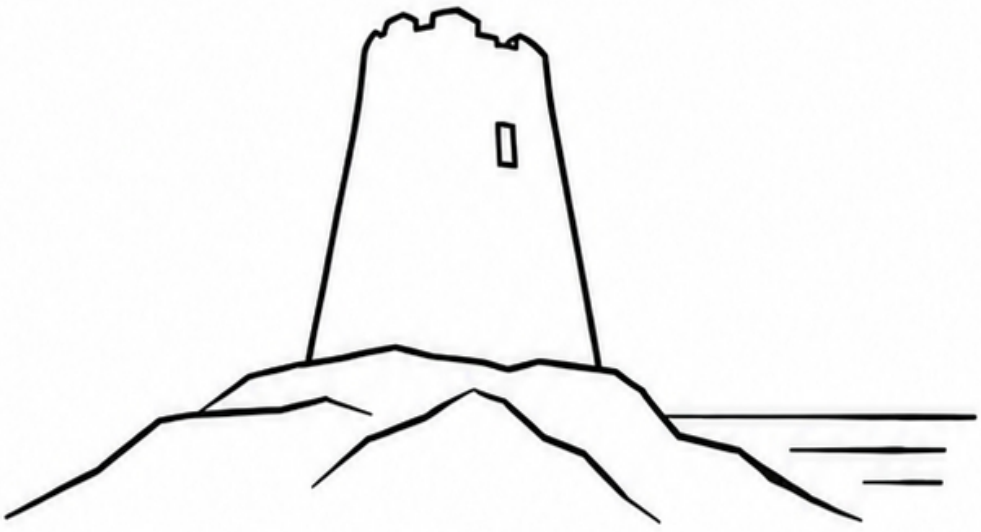
BETTER DECISIONS. LESS RISK.

A different model for advising government and defence on technology – advice that answers to no one but the truth.

June 2026



We create intelligent customers.

TABLE OF CONTENTS

Key Judgements:....3
Creating Intelligent Customers:....4
The current deficit:....4
Dependency sold as a feature:....5
Painted-on products:....6
Self-correction is impossible:....7
The intelligent customer:....8
Conclusion:....9
Author:....10
Sources:....11

KEY JUDGEMENTS:

1. Most consequential technology in government and defence is bought, built, and governed by people who do not understand it well enough to do all three safely. The deficit is not in the world's knowledge — the answers largely exist — but in its transfer to the people who carry the decision. *(High confidence. This is the formal finding of the National Audit Office, not only our observation.)*

2. The most damaging symptom of that deficit is **skills-lock**: a dependency on a small number of non-transferable people, often presented as a premium service rather than admitted as a defect. It is more dangerous than vendor lock because it does not appear on a balance sheet or bill of materials, cannot be cleanly audited, and cannot be exited without losing the capability itself. *(High confidence.)*

3. Buyers cannot reliably tell the real thing from the painted-on version — sovereign from foreign-hosted, assured from asserted, a finished product from funded research — because no party at the commercial table is paid to teach them the difference. The conflict is structural, not a matter of bad actors. *(High confidence.)*

4. The resulting cost is strategic, not only financial. It produces specifications that suppliers and adversaries can game, capabilities the state can neither see into nor leave, and a culture that has learned to read dependence as delivery. *(Medium-to-high confidence.)*

5. The remedy is a buyer competent enough to see through the next pitch — which requires at least one voice in the room with no reason to lie. In the current environment that has stopped being a desirable procurement preference and become a baseline security requirement. *(This is the paper's central claim. It is argued below, not asserted here.)*

CREATING INTELLIGENT CUSTOMERS:

Most consequential technology in government and defence is bought, built, and governed by people who do not understand it well enough to do all three safely. The people are rarely the reason. They are, in the main, capable and conscientious, working inside a system that hands them accountability without handing them legibility.

THE CURRENT DEFICIT:

A senior official is asked to approve a "sovereign cloud," a "zero-trust architecture," an "AI-enabled" platform — terms that arrive already carrying a supplier's preferred meaning, and that the official has no independent way to test. The responsibility is real. The comprehension is borrowed, almost always from the same people selling the thing, and these terms have rapidly become embedded in policy and doctrine.

This is usually diagnosed as a knowledge problem, and met with the usual remedy: more discovery, a longer scoping phase, another design team. That diagnosis is the expensive mistake. The knowledge is not missing. For most of what the state procures, the architecturally sound answer already exists and is well understood by practitioners. What is missing is its transfer — the unglamorous act of writing it down plainly enough that the person who carries the decision can hold it without help.

It is worth being clear that this is not a private opinion. The National Audit Office has reached the same conclusion in its own reviews, and named the missing capability precisely: the ability to act as an *intelligent client*. Its January 2025 review of government's approach to technology suppliers found that a lack of digital and commercial capability has wasted public money and stalled major programmes, that the public sector spends at least £14 billion a year on digital and technology, and that reliance on a handful of global providers for cloud and AI — services government does not ultimately control — now calls for a different approach.[1] The Public Accounts Committee put it more bluntly still: the centre of government has not helped departments become intelligent clients.[2] The diagnosis, in other words, is settled and on the record. What follows is about the cure.

The structure of the market quietly works against the customer. A great deal of what is sold as discovery, design, and embedded engineering exists not because the knowledge is absent but because transferring it plainly would end the engagement. A customer who held the pattern would not need the six-month design phase, the standing retainer, or the forward-deployed engineering team that has to stay forever. Almost everywhere the buyer turns, the incentive is to keep the knowledge resident in the supplier and rent it back. Dependence, in these arrangements, is not an accident. It is frequently the real product.

The cost of this used to be counted in money and time — a programme that ran long, a contract that delivered less than the brochure. That framing is now too generous. When the technology carries classified data, underpins an operational capability, or routes a nation's most sensitive information, not understanding what you have bought is no longer a value-for-money footnote. It is

an attack surface. The next two sections trace how the deficit becomes a vulnerability — first through dependency, then through illusion — and why the model that produced it cannot be the model that resolves it.

DEPENDENCY SOLD AS A FEATURE:

Take the clearest case first, because it is the one the industry has learned to present as a virtue.

A data-integration platform is procured for sensitive and classified work — often at speed, sometimes through a route that limits competition and later draws public and parliamentary scrutiny. The platform is genuinely sophisticated. It is also, in practice, unmanageable by the customer's own people. Making it work, and keeping it running, requires the supplier's engineers embedded alongside the live data, indefinitely. That embedding is not described as a limitation. It is sold as a premium service — proximity to the vendor's expertise, offered back to the customer as a benefit.

This is *skills-lock,* and it is worth being precise about why it is worse than the vendor lock everyone already knows to watch for.

Vendor lock is visible. It shows up in a contract, a switching cost, a line a finance director can point at. It is a poor bargain, but it is a legible one, and a competent buyer can price it and plan an exit. Skills-lock is none of those things. The dependency lives in people, not in a licence. It does not appear on the balance sheet in the same way. It cannot be audited as a cleanly defined risk, because there is no artefact to audit — the competence was never written down, and the customer's own staff were never brought up the curve. The system runs only so long as specific individuals keep it running, and when they are removed the capability is neither transferable nor salvageable. The state is left holding something it cannot operate, cannot modify, and cannot decommission on its own terms.

This is not a fringe concern, and again it is on the record rather than asserted. The Public Accounts Committee has found that less successful programmes were typically over-outsourced by departments with a thinly resourced internal client function, creating a dependence on external people who often had little knowledge of the existing systems.[2] The NAO's own guidance for audit committees asks the question that should be asked at the outset of every such purchase, and rarely is: if consultants or contractors are required to implement a system, will in-house staff be able to build capability alongside them?[3] When the honest answer is no, what has been bought is not a capability. It is a subscription to other people's competence.

Two further hazards compound this, and both are routinely underweighted at the point of purchase.

The first is that the people are not necessarily sovereign. A capability propped up by embedded engineers is only as sovereign as those engineers and the underlying jurisdiction they answer to. Where the platform's architecture also allows sensitive data to be observed, processed, or reached under a foreign legal regime, the

dependency stops being a resilience problem and becomes a counter-intelligence one. This is no longer hypothetical: in June 2025 a major US provider confirmed under oath to the French Senate that it could not guarantee sensitive data held in France against access under US law, even under a French-marketed "sovereign" offering.[4] By mid-2026 this had moved from concern to policy: in June 2026 the European Commission presented a Tech Sovereignty Package — including a Cloud and AI Development Act proposing tiered sovereignty requirements for sensitive public-sector workloads — while several European administrations were already moving off US platforms on sovereignty grounds.[5][6]

The second is that the dependency is broadly invisible until it is tested. A programme can look healthy for years — delivering dashboards, meeting milestones — while resting entirely on a foundation that cannot survive its own people leaving. The weakness surfaces at the worst possible moment: when the supplier is removed, the funding is cut, or the relationship sours, and the customer discovers that what they believed they had bought was a service that left when the people did.

Stated plainly: an arrangement like this is not a premium managed capability. It is an unfinished system, kept running by the people sent to compensate for the fact that it is unfinished, incomplete, or poorly suited — and when they leave, so does the capability. The test for it is simple, which is the point the rest of this paper builds toward: *if a system requires permanent boots on the ground to run, the system is broken.* A buyer competent enough to ask that question at the outset does not end up in such a position. The deeper trouble, addressed shortly, is that almost no one at the table has any reason to ask it on the buyer's behalf.

PAINTED-ON PRODUCTS:

The second failure is quieter than the first, because nothing visibly breaks. The customer simply buys something other than what they believed they were buying, and discovers the gap slowly.

A large provider sells a "sovereign, secure" environment to a public-sector customer as a finished product. It is not, in fact, a product. It is a bespoke development or integration that the customer is effectively funding the provider to build, and standing it up takes considerably longer than the sale implied. When it eventually runs, it turns out to be a constrained assembly of commodity infrastructure delivering a subset of what was specified and expected — and the headline capability that justified the premium, often an AI capability, arrives as a smaller, deployable model rather than the flagship the brand name evoked. None of this is necessarily dishonest. Each step is defensible on its own. The customer still ends up with something materially smaller and poorer than the thing they thought they were governing.

The reason this works is not that buyers are careless. It is that the words have been hollowed out. "Sovereign," "secure," "zero-trust," and "AI" arrive pre-loaded with the supplier's meaning, and the buyer has no independent instrument to test them against. The remedy is not more trust or more

caution. It is a small number of plain questions that collapse the gap between the claim and the thing, and that a competent buyer asks as a matter of routine:

- *Is this something you sell off the shelf, or are we funding you to build it?* — separates a product from research the customer is paying to de-risk.
- *Name another customer running this exact configuration in production.* — a claim that cannot survive this question was never a product.
- *When you say "sovereign," name the jurisdiction, the nationality of the operators, and who holds the keys.* — a European data-centre address changes the geography, not the jurisdiction; control follows the provider, not the building.[4][7]
- *When you say "AI," name the model, where its weights come from, and where inference runs* — not the brand family.

Each of these is a question a competent buyer asks and an under-equipped one does not. The distance between the two is the entire subject of this paper. None of the questions requires special clearance, secret knowledge, or a six-month engagement to ask. They require only that someone in the room understands the technology well enough to know which question matters — and has no reason to leave it unasked.

SELF-CORRECTION IS IMPOSSIBLE:

It would be comforting to treat the first two failures as the work of bad suppliers, to be solved by finding better ones. That is the second expensive mistake, and it is worth resisting carefully, because most of the people involved are neither dishonest nor incompetent.

Consider the commercial table as it is usually composed. The vendor is paid to sell the platform. The systems integrator is paid to deliver it, and earns more the longer and larger the delivery. The discovery consultancy is paid for the discovery, and is unlikely to conclude that little discovery was needed. Even the embedded engineers, doing genuinely skilled work, are paid for as long as the customer cannot do without them. Every one of these parties can be entirely honest and the customer can still end up dependent — because not one of them is paid to make the customer need them less. The conflict is structural. It does not require a villain.

This is not an argument that consultants add no value; many add a great deal, and government's own reviewers say as much.[8] It is an argument about what is structurally absent from the room. The NAO has noted that government does not even hold consistent data on how much it spends on external consultants — public-sector consultancy fee income has been estimated at over £5 billion a year — which makes the dependency hard to see, let alone manage.[8] You cannot govern what you cannot measure, and you cannot measure a reliance no one at the table is incentivised to name.

What is missing is a voice whose only product is the customer's understanding. Not a better-intentioned version of the existing parties — a structurally different one, with no platform to sell, no delivery to extend, no downstream stake in the answer. A voice that does not win if the customer buys, and wins only if the customer

understands. Its independence is not a matter of character; it is a matter of position. The advice can be trusted precisely because there is nothing downstream for it to protect.

THE INTELLIGENT CUSTOMER:

The cure follows directly from the diagnosis, and it is unglamorous. If the deficit is one of transferred competence, the remedy is to transfer it: to make the people accountable for a decision competent enough to buy, build, and govern the thing without renting their understanding from the seller. The national auditor named the missing capability the *intelligent client*. The work is to create it.

That is a narrower and more practical task than it sounds, because — to return to the founding observation — the answers largely already exist. The architecturally sound pattern for handling sensitive data in public cloud, for networking two systems so neither can observe the other, for testing whether a "sovereign" claim is real, is generally known to practitioners. It has simply never been written down for the person who has to sign the contract. Competence transfer is mostly the discipline of writing it down: in documents, not in heads; in language a minister and an engineer both follow; as an artefact the customer keeps, rather than a dependency the customer acquires.

Three things make such a voice trustworthy, and all three are matters of structure rather than goodwill:

It sells nothing downstream. No platform, no resale, no commission, no delivery contract waiting behind the advice. Independence is not a value statement; it is the absence of anything that could bend the answer.

It can be plain because it is independent. Plain words are only possible when no commercial interest depends on keeping things obscure. The ability to say a thing simply is, in this market, a reliable signal that the speaker has nothing to sell you.

And it does not need to be inside the secret to be useful — which is the part buyers find counter-intuitive, so it is worth stating deliberately and carefully. An adversary needs no clearance to attack you, and an independent adviser needs none to understand the threat. Clearance governs who may handle your data or see your processes; it has never been a measure of who understands either. The architecturally sound pattern is stronger than any single programme or classification, which means the right answer can be given without ever touching the classified specifics. Staying out of the secret is not a limitation on such a voice. It is what keeps its judgement clean.

For the senior reader, the practical implications reduce to a short list that can be acted on without waiting for anyone's permission:

- Treat competence as a deliverable. Require, in every significant engagement, a written artefact the customer keeps and can act on without the supplier in the room.
- Apply the plain-questions test before signing: product or funded research; another customer in production; jurisdiction, operators, and keys named; model and inference location named.

- Ask the boots-on-the-ground question at the outset, not at the post-mortem: if running it needs permanent embedded people, treat it as an incomplete solution until proven otherwise.
- Put one independent voice in the room on consequential decisions — one with no platform, no delivery, and no downstream stake. The cost of that voice is trivial against the cost of the dependency it prevents.

CONCLUSION:

None of the failures highlighted in this paper are secret, and none were bolts from the blue. Rather, they were foreseeable, and most were indeed foreseen. The capability gap was named in the public record by the national auditor before many of the cheques were signed. The sovereignty exposure was admitted, on oath, by the providers themselves. The pattern of dependency sold as a service has been visible to anyone willing to ask whether a system could survive its own people walking out of the door.

What was missing in each case was not knowledge. It was a voice in the room with no reason to stay quiet. The state is now paying for that absence twice — once to buy the dependency, and again to unpick it — and the second bill is the compound interest on top of the first mistake.

The argument of this paper is therefore modest in form and not at all modest in consequence. Buy, build, and govern from a position of understanding rather than borrowed comprehension, and the expensive mistakes mostly do not happen. The means is competence, transferred plainly and kept. The precondition is one honest voice with nothing downstream to protect. The result is better decisions and less risk — which is, in the end, the only thing any of this was ever about.

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.

SOURCES:

1. National Audit Office, *Government's approach to technology suppliers: addressing the challenges*, HC 616, Session 2024–25, 16 January 2025. Establishes public-sector digital spend of at least £14bn/year; a lack of digital and commercial capability; reliance on global cloud and AI providers whose services government "does not ultimately control"; and the recommendation that departments strengthen their "intelligent client function." The accompanying statement by PAC Chair Geoffrey Clifton-Brown noted the centre had not helped departments "become intelligent clients."
   https://www.nao.org.uk/reports/governments-approach-to-technology-suppliers-addressing-the-challenges/
2. Committee of Public Accounts, *Challenges in implementing digital change*, Thirtieth Report of Session 2021–22, HC 637, 10 December 2021 — on the C&AG's report *The challenges in implementing digital change*, HC 575, 21 July 2021. Finds that less successful programmes were typically over-outsourced by departments with a thinly resourced internal client function, creating dependence on external people with little knowledge of the existing systems.
   https://publications.parliament.uk/pa/cm5802/cmselect/cmpubacc/637/report.html
3. National Audit Office, *Guidance for audit committees on cloud services* (good-practice guide, 2019; accessible re-issue 2021), with related material in *Digital transformation in government* good-practice guidance, 2024. Sets the test of whether in-house staff can build capability alongside contractors, and the technical lock-in and portability trade-offs.
   https://www.nao.org.uk/wp-content/uploads/2021/04/Guidance-for-audit-committees-on-cloud-services-Accessible.pdf
4. Testimony of Anton Carniaux, Director of Public and Legal Affairs, Microsoft France, before the French Senate *commission d'enquête* on public procurement and digital sovereignty, June 2025 (Senate report N° 830, session extraordinaire 2024–2025). Asked under oath whether he could guarantee that French public-sector data would never be transmitted to US authorities without French consent, he answered: "Non, je ne peux pas le garantir." Illustrative of provider-control jurisdiction under the US CLOUD Act (2018).
   https://www.senat.fr/
   https://videos.senat.fr/
5. CNBC, *EU weighs restricting use of U.S. cloud platforms to process sensitive government data, sources tell CNBC*, 7 May 2026. The European Commission subsequently presented its Tech Sovereignty Package, including the Cloud and AI Development Act, on 3 June 2026.
   https://www.cnbc.com/2026/05/07/eu-commission-cloud-sensitive-data.html
   https://www.cnbc.com/2026/06/03/europe-tech-sovereignty-us-tech-reliance.html
6. Reporting on European public-sector moves toward digital sovereignty, 2025–26: Germany — Schleswig-Holstein migrating tens of thousands of public workstations off Microsoft to open source, citing data control and the CLOUD Act, with its CIO describing the migration period as acutely difficult (an illustration of real exit cost); Denmark — Ministry of Digital Affairs adopting open-source office software; Switzerland — data-protection authority guidance against international cloud services for personal data; France — government-developed tools replacing US services.
   https://www.theregister.com/2025/10/15/schleswig_holstein_open_source/
   https://www.raconteur.net/technology/schleswig-holstein-open-source
   https://cybernews.com/news/schleswig-holstein-germany-microsoft-open-source/
7. European Union, *Data Act* (Regulation (EU) 2023/2854), Chapter VII; and *General Data Protection Regulation* (Regulation (EU) 2016/679), Article 48. The instruments underpin the point that a European data-centre address changes the geography but not the jurisdiction — control follows the provider, not the building. *(Author's analysis of the primary texts.)*
   https://eur-lex.europa.eu/eli/reg/2023/2854 https://eur-lex.europa.eu/eli/reg/2016/679
8. National Audit Office, *Lessons learned: the government's use of external consultants*, 21 November 2025. Government lacks consistent data on consultancy spend; the Management Consultancies Association estimates public-sector consultancy fee income at £5.3bn (2023) and £4.6bn (2024); consultants and civil servants increasingly work in blended teams, often adding real value.
   https://www.nao.org.uk/wp-content/uploads/2025/11/governments-use-of-external-consultants.pdf

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

(nʊˈrɑːgeɪ)

Sovereign technology strategists
for government and defence.

We create intelligent customers.