Australian Government
Digital Transformation Agency

COORDINATED CONTRACT AGREEMENTS SUBMISSION TO ENABLE AUSTRALIA'S SOVEREIGN STRATEGY

STRONGER ECONOMY.
GREATER RESILIENCE.
SUSTAINABLE FUTURE.



Kitbag
ENTERPRISE EVOLVED

Suitability Assessment Framework for Coordinated Contracting Arrangements

Submitted by Kitbag Consulting and KB Technology

In response to: DTA Discussion Paper, June 2026 | Questions 2, 3, 4 and 5

About This Submission

This submission is made by Kitbag Consulting and KB Technology, an accredited Australian Early-Stage Innovation Company (ESIC) building digital capability in Australia, in response to the DTA's discussion paper on seller eligibility for coordinated contracting arrangements (CCAs). We provide views on Questions 2, 3, 4 and 5.

Preliminary Position: Australian Jurisdictional Risk

The US CLOUD Act[1] compels US companies to provide access to data and systems under their control regardless of where those systems are physically located, regardless of what the contract says and regardless of whether the Australian counterparty has consented. The vendor cannot override that obligation even if it wanted to. The contract does not supersede the law the vendor answers to.

China's National Intelligence Law[2] carries an equivalent obligation. Article 7 requires any Chinese organisation or citizen to support, assist and cooperate with national intelligence work. Article 14 grants Chinese intelligence agencies the authority to demand cooperation from any relevant institution. There is no opt-out provision, no contractual carve-out and no mechanism by which a Chinese-domiciled or Chinese-controlled entity can refuse a request from the state. This obligation follows the vendor into every relationship, regardless of where the subsidiary is incorporated, where the servers are located, or what the contract says.

A contract governed by Australian law does not extinguish these obligations. It coexists with them and when they conflict, the vendor's home jurisdiction prevails. Multinational vendors frequently promote sovereign cloud offerings based on physical data location. Physical location does not resolve jurisdictional exposure. In 2025, Switzerland formally rejected Palantir for sensitive military applications[3] not on capability grounds, but because the company's exposure to US jurisdiction meant Switzerland could not guarantee long-term sovereign control of its government data. Switzerland has also moved to restrict Microsoft as the predominant office suite across government operations[4] for the same reason. They are the considered conclusions of a neutral nation with a long history of institutional risk management.

[1] Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), 18 U.S.C. § 2713. Requires US-based technology companies to produce data stored outside the United States when served with a valid US legal process, regardless of where that data is physically located.

[2] People's Republic of China, National Intelligence Law (2017), Articles 7 and 14. Requires any Chinese organisation or citizen to support and cooperate with state intelligence work; no contractual carve-out or subsidiary structure can override this obligation.

[3] Swiss Armed Forces internal risk assessment (December 2024), reported by Republik and netzpolitik.org (December 2025). The 20-page evaluation concluded Palantir's US jurisdiction created an unmitigable sovereignty risk and recommended considering alternatives.

[4] Swiss federal and cantonal authorities, 2025–2026. A government feasibility study confirmed open-source replacement of Microsoft 365 is viable, citing US CLOUD Act exposure as a primary concern. See: lenews.ch and swissinfo.ch (April 2026).

The question governing a Commonwealth Contract for Capability is therefore not simply which terms and conditions apply. It is which jurisdiction controls the relationship when those frameworks conflict. A vendor domiciled in a foreign jurisdiction who accepts Australian T&Cs has not resolved that conflict.

The deeper risk is operational, not contractual. The problem is not simply that AI tools are foreign built. It is that the logic encoding how an organisation functions, how decisions are made, tasks executed and authority exercised, increasingly resides in platforms beyond Australian legal control. When government agencies embed their operational logic in foreign platforms, three structural vulnerabilities follow.

Kill Switch Risk

When the US sanctioned the chief prosecutor of the International Criminal Court, he lost access to his Microsoft cloud account overnight.[5]. Parts of national capability can be rendered inoperable by legal decisions taken in a foreign jurisdiction in which Australia has no standing and no recourse.

On 13 June 2026, the US administration-imposed export controls on Anthropic's Fable 5 and Mythos 5 models, cutting off access for every non-US user worldwide. Anthropic complied immediately. There was no warning, no transition period, and no Australian legal mechanism to prevent it or seek redress. Organisations that had embedded those models into their operations lost access overnight and critically, so did those operating through Anthropic's own Australian subsidiary. No local structure, no local contract, and no local relationship could override a directive from the foreign parent's home government. Australia had no standing, no vote and no recourse. It is the precise scenario this submission has sought to address: the strategic and operational exposure created when Australian institutions embed their workflows in foreign-controlled AI platforms whose continued availability is subject to legal, political and commercial decisions made in another country, in another interest, under another flag.[6]

Corporate Veil Risk

Multinational vendors answer to their global headquarters and foreign regulators. The PwC Australia scandal[7] illustrated this directly when the Senate sought critical information, PwC International refused on the basis that the material belonged to the global entity. A domestically owned vendor has no such conflict. Its obligations are singular and Australian.

Dependency shadow

Over time, agencies reshape their processes around dominant platforms and internal understanding of operational logic erodes. When substitution becomes necessary due to sanctions, policy divergence or strategic realignment the obstacle is not finding a comparable tool. It is restoring the sovereign capability that was allowed to atrophy. That restoration is expensive, slow and politically difficult precisely because the dependency was never formally acknowledged as a risk.

---

[5] US Executive Order 14203 (6 February 2025), sanctions on International Criminal Court personnel. Following the order, the ICC chief prosecutor lost access to Microsoft cloud services; the ICC subsequently migrated away from Microsoft to open-source alternatives, illustrating how foreign legal action can render organisational capability dependent on a foreign vendor's compliance decisions.

[6] Axios, 'Trump administration blocks foreign access to Anthropic's most powerful AI' (12 June 2026); ABC News, 'Trump administration forces Anthropic to pull models worldwide' (13 June 2026).

[7] Australian Senate Finance and Public Administration References Committee, PwC Australia inquiry (2023–2024). PwC International declined to provide documents to the Senate and ATO on the basis that material belonged to the global entity, not the Australian firm.

The answer is not better contract terms. It is selecting vendors whose legal domicile, operating infrastructure and accountability framework are subject to Australian law without qualification where no foreign statute exists to override what the contract says, and no foreign government holds a legal instrument compelling access to Australian operational systems.

There is no avoiding the fact that the geopolitical environment in which these procurement decisions are made is not stable and it is not improving. Commercial relationships are increasingly being weaponised as instruments of state leverage through tariffs, technology access restrictions, the threat of platform withdrawal and through legal compulsion mechanisms that were always present but are now being actively exercised.

Procurement risk assessment that does not account for the political disposition of a vendor's home jurisdiction and the instruments that jurisdiction holds over the vendor's obligations to Australian clients is not risk assessment. It is assumption management dressed as due diligence.

The decisions being made in procurement today will define the exposure Australian organisations carry for the next decade. The geopolitical environment demands that those decisions be made with full awareness of what jurisdiction follows the vendor through the door.

> *Australia is not alone. Germany mandates domestic jurisdiction over government IT*[8]. France enforces SecNumCloud[9]. Gaia-X[10] invests in federated sovereign infrastructure. Canada introduced a digital sovereignty procurement framework in late 2025[11]. Not moving in a comparable direction risk positioning Australia as an outlier not for lack of capability, but for misidentifying where sovereignty now resides.

[8] BSI IT-Grundschutz framework; German Federal Government cloud strategy. The state of Schleswig-Holstein migrated 40,000+ workstations to open-source software, achieving over €15 million in annual savings.

[9] ANSSI SecNumCloud qualification framework (France), ssi.gouv.fr. Sets mandatory sovereignty requirements for cloud providers serving sensitive French government data, including that operational control not be subject to non-EU legal jurisdiction.

[10] Gaia-X, European federated data infrastructure initiative, gaia-x.eu (est. 2019, Germany and France). Aims to create a sovereign, interoperable European cloud ecosystem reducing dependency on non-European technology providers.

[11] Government of Canada, Digital Sovereignty Framework, Treasury Board Secretariat (November 2025); Buy Canadian procurement policy framework (December 2025). The Framework outlines procurement and technical controls to strengthen institutional control over federal government data and systems. See: canada.ca

Question 2 — Terms and conditions

> *What risks or challenges does accepting government terms and conditions (rather than seller T&Cs) create for sellers and how could those challenges be addressed?*

Our Position

Kitbag Consulting and KB Technology accepts government terms and conditions as a baseline requirement. The risks and challenges of doing so are real but addressable provided the framework distinguishes between sovereignty terms, which are non-negotiable and commercial mechanics, which can be adapted proportionately to a seller's structure and risk profile. The tier framework below provides that mechanism.

Sovereignty Terms and Conditions

Sovereignty terms exist because Australian law cannot compel a foreign vendor's home government. Accepting Australian T&Cs on jurisdiction and data governance is the minimum condition for calling an arrangement sovereign. That condition applies regardless of vendor origin. The goal is not to exclude foreign vendors categorically but to ensure Australian options receive a fair hearing and that Australia's digital sovereignty is actively encouraged and protected. As Assistant Minister Charlton observed at UTS, Australian options are currently losing by default, not by merit.

Acceptance of Australian government sovereignty terms on jurisdiction, data governance and accountability to Australian law should be a condition of eligibility, not a starting position for negotiation. A seller's resistance to these terms is itself a sovereignty signal. It typically reflects an unwillingness to submit to Australian legal jurisdiction, a preference for contract terms drafted to protect foreign corporate interests, or a structural inability to separate Australian operations from the global policy frameworks their parent entity operates under. These are not administrative concerns; they are indicators of where control of the relationship resides.

For sellers subject to the US CLOUD Act[12] or comparable extraterritorial instruments, accepting Australian government terms on jurisdiction and data governance is the minimum necessary condition for the arrangement to function as described. The CLOUD Act compels US-incorporated companies to produce data held under their control regardless of where it is physically stored, regardless of what the contract says and regardless of whether the Australian counterparty has been notified or consented. An Australian contract that coexists with that obligation does not resolve, only defers the jurisdictional question. The terms the government accepts as sovereign protection may, in practice, be subordinate to a foreign statute the vendor cannot override even if it chooses to.

That baseline is not a burden to be negotiated away. It is the minimum condition for calling the arrangement sovereign. The jurisdictional dimension of this question is addressed in our preliminary position above.

[12] Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), 18 U.S.C. § 2713. Requires US-based technology companies to produce data stored outside the United States when served with a valid US legal process, regardless of physical location.

Commercial Terms and Conditions

We acknowledge that genuine operational challenges exist, particularly for sellers whose global structures were not designed around Australian procurement requirements. Liability exposure, IP provisions affecting global product deployment and conflicts with international compliance certifications are real friction points. These are not sovereignty issues; they are commercial ones, and they are addressable through standard contract negotiation practices.

Introducing the tier framework

Not all sellers present the same risk profile and a procurement framework that treats them identically will either exclude capable local suppliers through unnecessary friction or expose government to jurisdictional risk by applying the same flexibility to foreign-controlled entities. The tier framework set out in Question 3 addresses this by calibrating sovereign accountability to structural risk. It recognises that an Australian-owned business operating entirely under Australian law is a fundamentally different proposition from a transnational entity whose parent is subject to foreign government compulsion. The degree of commercial flexibility available under T&C negotiations should reflect that difference.

The World Economic Forum[13] defines digital sovereignty as the ability to have control over your own digital destiny the data, hardware and software that you rely on and create. International accounting standards[14] define *Control* of an economic resource meaning the ability to direct the use of the economic resource and obtain the economic benefits that flow from it. *Control* also includes the ability to prevent others from directing the use of and obtaining the benefits from the resource.

The WEF identifies multiple dimensions including data sovereignty, operational sovereignty, technical sovereignty and legal sovereignty. Critically, its 2026 framing rejects the false choice between sovereignty and openness: sovereignty means balancing strategic self-reliance with intelligent partnerships, not isolationism

Applying this to T&Cs, we propose a tiered framework that gives procurement specialists a mechanism to assess the risk profile of foreign entities, while preserving the underlying principles of sovereignty terms across all tiers and allowing commercial mechanics to be adapted proportionately. The goal is an Australian procurement function that does not just assess foreign risk but actively champions domestic capability.

Tier 1 — Australian-owned, subject only to Australian law These sellers face the least friction. Their structures are already aligned with government requirements and government T&Cs should apply with minimal adaptation.

Tier 2 — Australian-owned in collaboration with a foreign entity friction may arise where multinational arrangements introduce conflicting obligations. Commercial terms may be adapted proportionately to the nature and depth of the collaboration. A Deed of Sovereignty can help delineate which obligations sit with the Australian entity and which with the foreign partner, preserving sovereign accountability while acknowledging operational reality.

[13] World Economic Forum, 'Digital Sovereignty' (2025/2026), weforum.org. Defines digital sovereignty as "the ability to have control over your own digital destiny — the data, hardware and software that you rely on and create."

[14] IFRS Conceptual Framework for Financial Reporting (2018), paragraph 4.20, International Accounting Standards Board. Defines control as the present ability to direct the use of an economic resource and obtain the economic benefits that flow from it.

Tier 3 -- Foreign entity with Australian subsidiaries A defined set of commercial carve-outs may be negotiated where genuine conflicts with global structures exist, subject to disclosure to the relevant agency and approval. These carve-outs apply to commercial mechanics only, not to jurisdiction, data governance, or accountability provisions.

Tier 4 — Transnational Platforms/Sellers Government T&Cs apply in full as a condition of eligibility. Their jurisdictional exposure is precisely the risk the T&Cs are designed to manage and no commercial carve-out resolves that underlying problem.

Introducing the Deed of Sovereignty

The Deed of Sovereignty is a proposed instrument to address a structural limitation in current procurement frameworks: that accepting Australian T&Cs does not extinguish a foreign vendor's obligations to its home jurisdiction. A contract governed by Australian law coexists with, but does not override, the statutory obligations a vendor carries by virtue of its domicile. Where those obligations conflict, the vendor's home jurisdiction prevails. No commercial negotiation resolves that. The Deed works by making sovereign accountability an explicit, standalone commitment, delineating which obligations sit with the Australian entity, which sit with the foreign partner, and how conflicts between them are resolved. It operates at a different layer from standard T&Cs: where T&Cs govern the commercial relationship, the Deed governs the sovereign one. It is designed to operate within existing Australian contract law and deed instrument precedent, requiring no new legislative framework to implement. For Tier 2 arrangements, where an Australian-owned entity collaborates with a multinational, the Deed provides the mechanism to preserve sovereign accountability at the Australian layer while acknowledging the operational reality of the partnership. For Tier 3 arrangements, it functions as a condition of eligibility, a binding commitment that jurisdictional exposure has been identified, disclosed, and allocated. It does not eliminate foreign jurisdictional risk where that risk is structural. What it does is make that risk visible, named, and governed, shifting it from an assumed condition of the arrangement to an explicit and auditable obligation.

The Distinction in Practice

The framework above draws a clear line: commercial terms can be adapted to build a workable, sustainable supplier relationship. Sovereignty terms cannot. This distinction allows government to engage pragmatically with the market without compromising the accountability and jurisdictional integrity that Australian procurement policy is designed to protect.

Question 3 — Broader economic benefits & public reporting

> *Thinking about the broader economic benefits that CCA sellers may provide to the Australian economy, what offerings are commercially reasonable from your perspective and what should be included in public reporting to provide transparency whether planned economic benefits have been achieved?*

Our Position

The PGPA and the Commonwealth Procurement Rules should embed a sovereignty weighting into the value for money evaluation, following New Zealand's precedent of a legislated minimum 10% weighting on sovereign capability. The case for doing so is economic as much as strategic. The existing SSA structure has defaulted to sellers already holding significant government presence, which in practice are large foreign multinationals that use transfer pricing and intra-group arrangements to repatriate profits to their parent jurisdictions. Commonwealth expenditure that appears to support domestic capability is in substantial part flowing offshore. A sovereignty weighting distinguishes between spending that circulates within the Australian economy and spending that does not. Value for money with a sovereignty dimension should therefore be the organising principle that separates genuine economic contribution from contractual window-dressing.

The independent review of the government's Single Seller Arrangements found that while the arrangements have driven reported savings of $1.6 billion, realised discounts are "hard to quantify", actual license use has "limited visibility", and some arrangements operate as simple commercial transactions rather than genuine strategic partnerships between government and industry. The review also found inconsistency between seller terms and government policy on cyber and local industry participation. The CCA suitability assessment framework is the mechanism to address those shortcomings and this submission offers a structured approach to doing so.[15].

What Is Commercially Reasonable to Expect

The following are reasonable baseline expectations of any CCA seller, calibrated to their sovereignty tier (see scale below):

- Investment in Australian operations across the full AI lifecycle, data infrastructure, GPU/inference, foundation models, applications and governance not just sales and account management presence.
- Full supply chain and jurisdictional disclosure: where model weights and operational logic are held, which foreign entities have legal access and whether the company is subject to instruments such as the US CLOUD Act, which compels US companies to grant access to data regardless of where it is physically stored.
- Data localisation for Commonwealth data as a baseline, including GPU inference onshore. Many transnationals route inferences through global AI factories; a user's request, potentially with attached Commonwealth data, is processed offshore even where storage is local. This must be explicitly confirmed and reported.
- Architectural separation between execution infrastructure (which can be globally shared) and operational ontology the logic encoding how an agency functions, complies and exercises authority. That layer must remain under Australian ownership and jurisdiction.

[15] Joseph Brookes, 'Govt agencies may team up on large tech procurements', InnovationAus (13 June 2026), innovationaus.com.

- Meaningful Australian SME subcontracting, with defined minimum thresholds as a share of contract value.
- Open-architecture or interoperability commitments ensuring the government can substitute execution layers without losing institutional knowledge operational IP must accumulate as a sovereign asset, not a platform dependency.

Proposed Sovereignty Scale for CCA Assessment

We propose the DTA adopt a four-tier sovereignty scale as a core assessment tool, reflecting the WEF's four sovereignty dimensions. The scale moves CCA assessment from binary eligibility to a graduated framework that rewards Australian-controlled capability and applies proportionate scrutiny to foreign dependency risk. Positioning within each tier is determined by two axes: sovereign control (legal, operational and jurisdictional) and Australian economic contribution (employment, R&D, SME participation, profits retained onshore).

Proposed Australian Economic Sovereignty Scale for CCA Sellers

TIER 1	**Fully Australian sovereign — preferred** ▲ Preferred • Australian-owned entity; IP, profits and operational logic retained onshore under Australian law. • Local workforce, R&D and engineering across the full AI stack — not just sales presence. • No foreign jurisdictional exposure; auditable build chain and model training practices. • Data, GPU inference, model weights and application layer all onshore.
TIER 2	**Australian-owned, in collaboration with a Foreign Entity — preferred with conditions** ▲ Preferred with conditions • Australian-owned and governed; primary accountability anchored in Australian law. • Collaboration with a multinational introduces some foreign dependency the nature and extent of that dependency determine positioning within this tier. • Sovereign control rating varies infrastructure partnership carries less risk than deep model or IP integration. • Deed of Sovereignty recommended where multinational collaboration creates material jurisdictional exposure.
TIER 3	**Foreign Entity with Australian subsidiary — conditional** ► Conditional • Foreign parent entity; IP and operational logic subject to foreign jurisdiction (e.g. US CLOUD Act). • Some onshore economic benefit through local operations, employment and tax contribution. • GPU inference path must be confirmed onshore — not routed through offshore AI factories. • Eligible subject to local benefit commitments, supply chain disclosure and Deed of Sovereignty.

TIER 4	**Fully Foreign Entity, no Australian benefit — high scrutiny** ▼ High scrutiny • No substantive local entity, workforce, or economic contribution to Australia. • Data, logic, IP and profits held offshore; full CLOUD Act and foreign regulatory exposure. • Operational kill switch sits outside Australian jurisdiction. • CCA eligibility requires exceptional justification and mandatory sovereign safeguards.

Tier 1 and Tier 2 sellers receive streamlined assessment. Tier 4 sellers face enhanced conditions or exclusion. Positioning within each tier is determined by the nature of the seller's arrangement, sovereign control and economic contribution are assessed across both axes.

Sovereignty Scoring Table

The World Economic Forum defines digital sovereignty as the ability to have control over your own digital destiny the data, hardware and software that you rely on and create. This scoring table operationalises that definition for CCA procurement assessment across two axes: sovereign control (60% of total score) and Australian economic contribution (40% of total score).

Score each criterion 0 (no / fully foreign), 5 (partial / conditional), or 10 (yes / fully Australian). Multiply each score by its weight to calculate the weighted contribution, then sum all contributions for the final sovereignty score out of 100. Contract value should also be considered: a vendor who qualifies at Tier 2 for a $30M contract may require Tier 1 safeguards at $200M, because the strategic dependency created by a larger arrangement amplifies every jurisdictional risk.

Criterion	Weight	Score (0 / 5 / 10)	Weighted score	Max possible	Notes
No foreign jurisdiction exposure US CLOUD Act, extraterritorial legal exposure. Physical location is not legal protection foreign governments can compel access to data regardless of where it is stored.	20%			20	CLOUD Act, extraterritorial legal exposure
Onshore operational logic the structured logic governing decisions, workflows and authority is a sovereign asset. When embedded in foreign platforms it becomes subject to foreign subpoena, sanction, or commercial change.	18%			18	Decision logic, workflows, governance
Australian ownership Domestic vendors have no conflict of interest between Australian obligations and foreign parent obligations. A Deed of Sovereignty can partially mitigate but not fully replicate this for foreign-parented vendors.	12%			12	No foreign parent with controlling interest
Data & inference localisation GPU inference processing must be confirmed onshore, not just data storage. Many platforms route inference through global AI factories, processing Commonwealth data offshore.	10%			10	GPU inference confirmed onshore

Criterion	Weight	Score (0 / 5 / 10)	Weighted score	Max possible	Notes
Australian workforce & R&D Skills and knowledge that develop within Australian-owned businesses stay within the Australian economy. This retention is structural and compounds over time it is the sovereign workforce dividend.	14%			14	Engineers, researchers not just sales
IP retained in Australia Operational ontologies and institutional logic must persist as Australian-owned assets, independent of any single model or vendor. IP held offshore migrates sovereignty with the platform.	12%			12	No IP transfer to foreign parent
Profits retained onshore Economic returns flowing to a foreign parent signal misaligned long-term interest. Onshore profit retention indicates the vendor's commercial future is anchored in Australia.	8%			8	Tax and financial returns in Australia
SME subcontracting CCA arrangements represent collective buying power at scale. Directing that power toward vendors with Australian SME supply chains multiplies sovereign economic benefit beyond the primary contract.	6%			6	Defined Australian SME thresholds
Total sovereignty score	**100%**		**/100**	**100**	

Tier guidance: 75–100 = Tier 1 (fully Australian sovereign) | 55–74 = Tier 2 (Australian, foreign entity collaboration) | 28–54 = Tier 3 (foreign entity with Australian subsidiary) | 0–27 = Tier 4 (transnational platforms). Contract value may lower the effective score threshold for higher tiers.

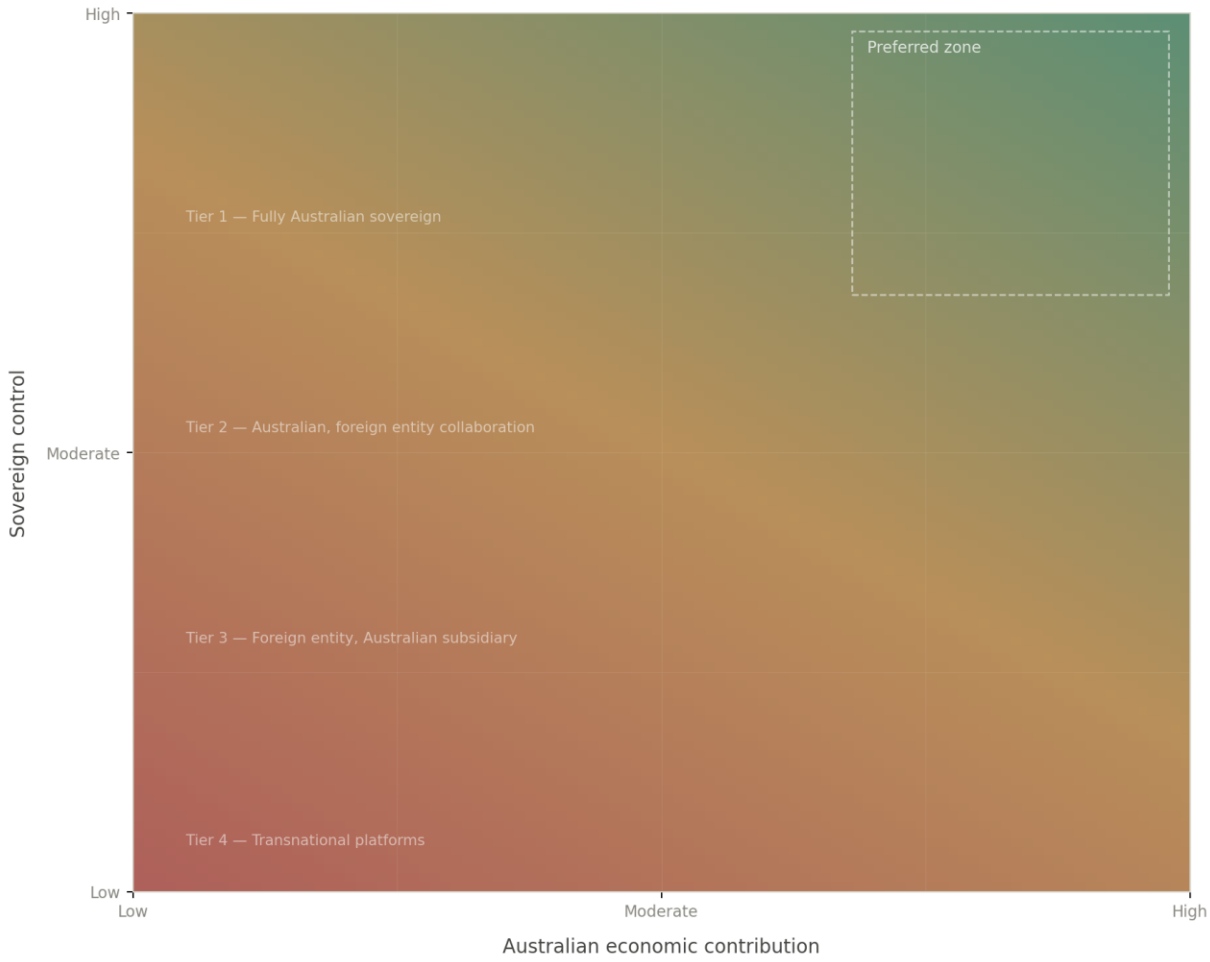


Figure 1: CCA seller sovereignty assessment matrix — sovereign control vs Australian economic contribution

What Should Be Publicly Reported

Annual reporting by CCA sellers, published on BuyICT, should cover:

- Total Australian spend including full supply chain breakdown
- Local employment by role type, distinguishing engineering and R&D from sales and support
- Australian SME subcontracting volumes as a percentage of contract value
- Sovereignty tier classification and any changes during the reporting period
- GPU inference path disclosure confirmation that Commonwealth data inference is processed onshore.
- Jurisdictional exposure summary: which foreign legal instruments apply to the seller's data and operational logic
- Deed of Sovereignty status where applicable
- Nature and extent of any multinational collaboration arrangements (for Tier 2 sellers)
- Progress against any sovereign capability commitments made at CCA establishment

We further recommend the DTA introduce a sovereignty maturity indicator distinguishing sellers who are contractually compliant from those who actively reduce the government's structural dependency on foreign-controlled digital infrastructure.

Question 4 — Digital skills & workforce development

> *What could CCA sellers do to help the public sector achieve the government's digital skills objectives? Consider short, medium and long-term objectives, as well as the opportunity to leverage a CCA to achieve outcomes for the government at scale rather than solely with individual agencies.*

Our Position

The DTA should distinguish between two fundamentally distinct workforce dynamics depending on seller sovereignty tier. For Tier 1 and Tier 2 sellers Australian-owned businesses employing Australians the question is not about training obligations. It is about the natural economic dividend of sovereign capability: skills, institutional knowledge and specialist AI expertise that develop within these businesses stay within the Australian economy. That retention is structural, not contractual. It compounds over time. When government procures from an Australian-owned business, it is investing in an ecosystem where the talent, the IP and the accumulated operational knowledge all remain here.

For Tier 3 and Tier 4 sellers, the dynamic is reversed. Skills developed in their engagements flow to global teams. IP accumulates offshore. The Australian economy receives a service, not a capability. For these sellers, explicit training and labour development obligations are not optional extras, they are the partial offset for the sovereign value that their structure cannot deliver by default.

> *Minister Charlton's observation that competitive advantage in AI now sits between the base model and the end product has a direct workforce implication: the skills that matter most are not those required to operate a vendor's interface, but those required to build and govern the layer above it — the agency's own operating logic, decision authorities and knowledge structures.*

Tier 1 And Tier 2 Sellers: Sovereign Skill Retention

The CCA framework should recognise and reward the structural workforce dividend that Tier 1 and Tier 2 sellers deliver. When government awards a CCA to an Australian-owned business, it is:

- Retaining specialist AI skills within the Australian economy rather than exporting them to a foreign parent's global talent pool
- Building a domestic base of engineers, researchers and practitioners who understand the Australian operating context the legislative environment, governance requirements and policy constraints that foreign models fundamentally lack
- Creating conditions for skills to compound: the more Australian businesses build AI for Australian government, the deeper and more capable the local talent ecosystem becomes
- Reducing long-term dependency on foreign expertise for the maintenance, governance and evolution of critical government systems

For Tier 2 sellers, the extent of this dividend depends on the nature of the multinational collaboration. Where the collaboration is at the infrastructure or execution layer, the core skill and knowledge retention benefit remains intact. Where it extends to IP or model development, the DTA should seek disclosure of where that knowledge resides.

The DTA should reflect this structural benefit explicitly in the sovereignty tier weighting it is the difference between an AI investment that builds national capability and one that rents it.

Tier 3 And Tier 4 Sellers: Explicit Development Obligations

For sellers who cannot deliver sovereign skill retention by structure, the CCA framework should require explicit labour and skills development commitments as a condition of eligibility, assessed across three horizons:

- **Short-term:** Free or heavily subsidised access to broadly transferable digital skills training, available whole-of-government rather than negotiated agency by agency. Aligned to Skills Framework for the Information Age frameworks (SFIA) and APS Professions standards not product certifications. Must include AI governance literacy: how to evaluate supplier sovereignty claims, audit supply chains across the AI stack layers, assess CLOUD Act exposure and govern deployed models.
- **Medium-term:** Co-design of nationally recognised, portable micro-credential pathways with the APS Academy, TAFE, or universities in cloud architecture, data engineering, cybersecurity, agentic AI governance and operational logic design. Capability that survives a model deprecation, vendor repricing, or foreign export control decision.
- **Long-term:** Structural knowledge transfer: open documentation standards, interoperability commitments and transition support ensuring institutional logic stays with the agency, not the platform. The goal is an APS that can substitute any execution layer or model without loss of operational knowledge. Sovereignty cannot be restored on demand. It must be designed in from the start.

What Should Be Publicly Reported

We recommend the DTA requires CCA sellers to report annually on:

- For Tier 1 and Tier 2 sellers: Australian headcount growth, role types created and R&D investment as evidence of the sovereign skill retention dividend. For Tier 2 sellers, disclosure of where knowledge generated through multinational collaboration resides.
- For Tier 3 and Tier 4 sellers: total training hours delivered, split by vendor-specific versus vendor-neutral content the ratio is a direct indicator of whether sellers are building sovereign capability or consolidating ecosystem dependency.
- Number of APS staff trained, by agency and role level and nationally accredited qualifications or micro-credentials delivered.
- Training content mapped against APS Professions standards and SFIA frameworks.

Question 5 — Other matters for the DTA's consideration

Are there any other matters that you consider should be included when the DTA is determining the principles for CCAs? Please feel free to provide your feedback or add your views.

Sovereign Systems of Work as a Mandatory CCA Procurement Category

The preceding answers concern the sellers an agency contracts. We close on the layer beneath that relationship, which the framework does not yet address: an agency's own operating logic, meaning the decisions, sequencing, approval authorities and policy associations that constitute how it functions. This logic exists independently of any system, and historically it has lived in legislation, policy, delegations, procedure and the experience of staff. When an agency undertakes a large platform deployment, an enterprise resource planning system or, increasingly, an artificial intelligence capability, a codified version of that logic is configured into the vendor's system. Where that layer sits inside a foreign-controlled platform, the dependency carries the jurisdictional exposure set out in our response to Question 3.

Beyond the issue of sovereignty, as an agency's operating logic accumulates inside a configured platform which it does not control, and the originating knowledge is not deliberately retained as a separable asset, the agency progressively loses the ability to operate, audit or replace that platform without the vendor. This dependency is well documented in Australian government, and its cost is a matter of public record. The whole-of-government GovERP program, which sought to standardise corporate systems across roughly one hundred agencies on a single enterprise platform, was wound back after expenditure the Minister for Finance described as almost $400 million, and was decommissioned in January 2025.[16] The Queensland Health payroll replacement required over 2,500 system customisations to encode the department's pay rules, affected the pay of tens of thousands of staff, and was estimated by the subsequent Commission of Inquiry to cost in the order of $1.2 billion to rectify and operate over eight years.[17]The Department of Defence is presently consolidating around five hundred applications onto a single enterprise resource planning platform at a cost valued in the billions, a program still in delivery.[18] These programs differ in their particulars, and together they show one pattern: once an organisation's operating logic is concentrated inside a large enterprise platform, substitution becomes slow, expensive and difficult to reverse.

The protection against this is architectural, and we describe it here as a sovereign System of Work. It is a layer that holds an agency's operating logic above and separate from the systems that execute it, under the agency's own ownership and Australian jurisdiction. Its value lies in what that separation makes possible. Execution-layer systems, whether an enterprise resource planning module, an artificial intelligence model or a productivity tool, can be substituted without the operating logic being lost alongside them. The logic itself remains inspectable and governable, which is the condition on which accountable AI deployment depends. The institutional knowledge of how the agency functions is retained as a sovereign asset rather than dispersed among vendors and consultants, and interoperability across systems is preserved because the logic connecting them is held in one governed place.

[16] Digital Transformation Agency, *GovERP Reuse Assessment* (August 2024), dta.gov.au. Finance Minister Katy Gallagher described the program as a costly flop based on "naive ideas about the ability to standardise complex corporate systems" after expenditure of approximately $390 million.

[17] Queensland Health Payroll System Commission of Inquiry, Final Report, The Honourable Richard N Chesterman AO RFD QC (31 July 2013), healthpayrollinquiry.qld.gov.au.

[18] Department of Defence, Defence Enterprise Resource Planning Program, defence.gov.au. Program consolidating approximately 500 legacy applications onto SAP S/4HANA; still in delivery.

The sequence in which this layer is established determines whether it protects anything. To preserve sovereignty over their operating logic, agencies should have a sovereign System of Work in place before they undertake large technology transformations such as enterprise resource planning deployments and artificial intelligence initiatives. Where the layer exists first, those subsequent procurements draw from and reference the agency's own logic, and the vendor systems are configured from it and do not become its only record. Where the layer is absent, each major platform reconstructs the operating logic inside itself, and command of that logic is conceded by default, one deployment at a time.

This points to a specific role for the framework. We recommend the DTA recognise the System of Work as a defined capability within the Australian Government Architecture, so that major enterprise resource planning and artificial intelligence investments, assessed through the Digital and ICT Investment Oversight Framework, are expected to demonstrate that the agency retains a sovereign operating-logic layer. We further recommend the DTA establish a System of Work category within the existing Software and ERP Marketplace, so that sovereign options in this category receive a structured procurement pathway rather than being assessed indirectly, if at all, through procurements scoped around other systems.

Recognised this way, the System of Work is both an architectural foundation and a procurement consideration in its own right. The framework can continue to assess sellers system by system, leaving the more consequential question of who commands an agency's operating logic unasked. The alternative is to make that question explicit, and to give agencies a sovereign means of answering it before their operating logic is committed to systems they do not control.

Closing Remarks

The tier framework, the sovereignty scoring table, the Deed of Sovereignty, the reporting requirements and the Systems of Work procurement category proposed in this submission are not independent measures. They are a single argument made at five levels: that sovereignty is a legal and structural condition, not a contractual one; that the vendor's domicile determines the jurisdiction that follows them through the door; that operational logic is a sovereign asset that must be governed as such; and that the CCA framework is one of the most direct instruments available to make Australian capability the default rather than the exception.

Sovereignty is not a passive state. It can be lost through accumulated deference as surely as through any single decision. The decisions being made in procurement today will define the exposure Australian organisations carry for the next decade. The framework should be designed to find Australian capability and to keep it here.