AUSTRALIAOS

DECISION INFRASTRUCTURE FOR AUSTRALIAN INSTITUTIONS

australiaos.com.au

CLASSIFICATION | RELEASED—DECISION SUPPORT

STRUCTURAL EXPOSURE ASSESSMENT · NO.002

Broadcom Structural Exposure *Assessment*

A jurisdictional assessment of Commonwealth dependence on VMware products contracted through corporate entities controlled by Broadcom Inc.

REFERENCE	DATE	CLASSIFICATION	VERSION
AOS-BCM-2026-002-v1.1	June 2026	Released	1.1

Contents

About this assessment

This is the second structural exposure assessment published by AustraliaOS. The first, AOS-TEL-2026-001, was a jurisdictional exposure assessment of Telstra under the Security of Critical Infrastructure Act 2018. This assessment applies the same methodology to Commonwealth dependence on VMware products contracted through corporate entities controlled by Broadcom Inc.

The assessments are published as public demonstrations of a methodology that AustraliaOS makes available to institutional buyers on a paid basis. The methodology produces structural exposure findings traceable to primary sources, with each factual claim verified against a public primary source and independently checkable by the reader. The category of exposure assessed sits outside the scope of the Information Security Manual and the Information Security Registered Assessors Program, which assess security controls rather than the legal authority of a vendor's home jurisdiction.

The intended reading audience is institutional decision makers responsible for vendor selection, procurement, and risk acceptance in Commonwealth agencies, oversight bodies, and the wider Australian institutional environment.

This assessment is decision support. It is not statutory authority and not a substitute for individual agency risk assessment. The reader is the decision maker.

01 Legal framework

This section fixes the statutory and legal boundaries within which this assessment is made.

Broadcom is the controlling US incorporated parent

Broadcom Inc (NASDAQ: AVGO) is a Delaware corporation. Effective 4 April 2018, a new Delaware parent, Broadcom Inc., replaced the Singapore parent, which became a subsidiary. This completed in the same period that Broadcom's CFIUS reviewed acquisition of Brocade Communications Systems closed, on 17 November 2017. Broadcom states the move to the United States was undertaken as part of the Brocade clearance; an independent analysis characterises it as a strategic relocation. On either account, Broadcom is a United States incorporated company within CFIUS reach. Broadcom is the parent of VMware LLC (Delaware) and VMware International Unlimited Company (Ireland), both wholly owned subsidiaries named in Broadcom's SEC filings. VMware Australia Pty Ltd (NSW) is wholly owned through the Irish parent.

The contracting relationships under which Australian Commonwealth agencies receive VMware products sit with the Australian and Irish subsidiaries. Ultimate corporate control sits with Broadcom Inc.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

United States control creates distinct categories of exposure

United States law provides several mechanisms that, on their terms, apply to a US controlled vendor and its foreign subsidiaries, but those mechanisms do not all reach the same thing. They fall into three categories, which this assessment keeps distinct because conflating them overstates the data access risk and understates the others.

Data access. Section 2713 of the Stored Communications Act, as amended by the CLOUD Act in 2018, provides that a covered electronic communication or remote computing service provider must disclose data within its possession, custody, or control on United States legal process, regardless of where the data is held. Because that test turns on possession, custody or control rather than location, the question for a subsidiary is whether the United States parent has practical control of the data, not where the data sits. Both turn on the same conditions: that the provider is one the relevant law covers, and that it holds or controls the data. For hosted services those conditions may be met; for software an agency runs on its own systems, they may not be.

Supply continuity. United States export control and sanctions regimes, administered under the Export Administration Regulations by the Bureau of Industry and Security and by the Office of Foreign Assets Control, apply to United States controlled vendors and their foreign subsidiaries and govern what those vendors may supply, to whom, and where. These regimes do not reach data; they bear on the vendor's ability to continue serving a customer.

Corporate control. CFIUS jurisdiction over Broadcom is established. In the same period as its CFIUS reviewed acquisition of Brocade Communications Systems, Broadcom completed its move to a United States parent; Broadcom states this was undertaken as part of the Brocade clearance, while an independent analysis characterises it as a strategic relocation. This regime governs ownership and transactions rather than data, and establishes that the United States government reviews the vendor's transactions under national security authority.

The CLOUD Act Agreement does not resolve the data access question

The Australia-United States CLOUD Act Agreement, made under section 2523, governs reciprocal access between Australian and United States authorities. It administers how cross border requests are handled. It does not narrow whatever Section 2713 obligation a covered United States provider owes to United States legal process, and it does not create one where the statutory conditions are not met. Section 2523, which authorises the Agreement, establishes a separate framework for reciprocal access and contains no provision narrowing the Section 2713 obligation owed by a covered US provider (CLAIM P). The Agreement is therefore not the variable that determines data access exposure. The variable is whether, for a given contract, the vendor is a covered provider holding the data at all, which the Agreement does not address.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

ISM and IRAP are the reference baseline

The Information Security Manual produced by the Australian Signals Directorate (through its Australian Cyber Security Centre) sets the technical control baseline for Australian Government information systems. The Information Security Registered Assessors Program provides independent assessment of systems against the ISM. Together, ISM and IRAP set the standard for how Australian agencies evaluate the security of cloud and ICT services.

The ISM is a cyber security framework of controls for protecting information technology and operational technology systems from cyber threats. IRAP provides independent assessment of systems against those ISM controls. Their stated scope is cyber security; the legal authority a vendor's home jurisdiction can exercise over the vendor falls outside that stated scope.

Framework position

Broadcom is a Delaware corporation, subject to United States jurisdiction. Its Australian and Irish subsidiaries hold the Commonwealth contracting relationships. Whether Commonwealth data held in connection with those contracts is reachable through the United States parent depends on the conditions set out above: whether the relevant law covers the service as provided, whether the data is in a provider's possession or control, and how the software is deployed. Those conditions are not established by the procurement record and vary across the contract estate. The exposure is therefore not uniform and not automatic. It is a set of distinct, partly conditional risks that no current framework requires anyone to assess.

02 Case context

The case subject is the Australian Commonwealth's concentrated dependence on VMware products contracted through corporate entities ultimately controlled by Broadcom Inc. The assessment scope is the foreign legal access exposure created by US corporate control over the VMware supplier entities used across the Commonwealth, measured against the analytical baseline of ISM and IRAP and the structural exposure category those frameworks do not cover. The exposure is concentrated, not distributed. Between 13 May 2023 and 13 May 2026, 113 Contract Notices published on AusTender record AUD 694,715,987 (approximately $694.7 million) in Commonwealth spending with Broadcom controlled VMware entities, across 22 agencies including the Department of Defence, the Australian Taxation Office, Services Australia, the Department of Home Affairs, the Reserve Bank of Australia, and the Australian Federal Police. One of the 113 contracts is a $13,075 training membership with VMware User Group Inc, a user community rather than a Broadcom controlled entity. This contract is included in the aggregate counts but sits outside the corporate chain analysis that follows. The contracts are public. The corporate chain is public. The concentration is the operational fact this assessment addresses.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

03 Assessment summary

The Commonwealth has placed AUD 694,715,987 of dependence on a single United States controlled software vendor: 113 Contract Notices, 22 agencies, the period 13 May 2023 to 13 May 2026. That figure is the supply continuity and corporate control surface: it does not depend on deployment, it does not turn on whether the CLOUD Act reaches any particular contract, and it attaches in full to the corporate chain established in section 01 (ANALYSIS B).

The data access surface is structurally different. CLOUD Act Section 2713 reach depends on whether the vendor holds the data, which depends on how the software is deployed (ANALYSIS A). The published procurement record settles this question for only a small subset of the estate.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

4.3 % Section 2713 floor · 15.6 % cleanly self run · 80.1 % residual indeterminate (of which 39.2 % is the undisclosed-deployment sub-band on the two largest contracts)

BAND	VALUE (AUD)	NOTE
Section 2713 floor	29,629,247.49	Nine contracts whose titles or categories unambiguously name a vendor operated hosted service (Software as a Service, Cloud Foundation, CloudHealth, Cloud on AWS). For these the Section 2713 precondition that the vendor hold the data is most plausibly met.
Cleanly self run	108,680,410.66	A single contract, the Australian Taxation Office's three year CN4142919-A1 covering licences for CA Mainframe and VMware products. This is the largest contract whose published title discloses enough to support a defensible inference that the agency runs the software on its own infrastructure and holds its own data.
Residual indeterminate against Section 2713	556,406,329.30	(total dependence minus the Section 2713 floor minus the cleanly self run band). Composed of: • AMBIGUOUS cloud / subscription sub band: 15 contracts, AUD 96,791,665.39, titled "Software Subscription" without disclosing whether hosted or licensed. • support / maintenance class: AUD 92,068,878.64, which does not raise Section 2713 questions in its own terms. • professional services class: AUD 3,535,803.09, which does not raise Section 2713 questions in its own terms. • undisclosed deployment on the two largest contracts: AUD 272,235,934.72 — the Department of Defence ($178,086,239.95, CN4211096) and Services Australia ($94,149,694.77, CN4071834-A1), together 39 per cent of total spend, each carry an AusTender Description field of exactly one word: "Software"; the public record does not distinguish whether these contracts host or licence. • generic-titled balance, ranks 4–51 unclassified in this report: AUD 94,089,468.14 across lower-ranked generic contracts. • less small overlap from multi-class contracts: (AUD 2,315,420.68).

The methodology that produced these figures is set out in section 06; the per contract resolution underlying the floor and the undisclosed deployment band is recorded in the verification harness, in GENERIC-CLASSIFICATION-2026-05-30.md.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

The structural finding of this section: the Commonwealth cannot determine its own data access exposure from its own publicly available procurement records (ANALYSIS C). The supply continuity and corporate control exposure surface attaches in full to the AUD 694,715,987 figure regardless of deployment (ANALYSIS B). The data access exposure surface has a published floor of AUD 29,629,247.49, a published cleanly self run band of AUD 108,680,410.66, and an undisclosed deployment indeterminate band that includes the Commonwealth's two largest VMware contracts. The structural exposure assessed in this document is not made up of two precise figures; it is made up of a firm supply and corporate control floor against the entire estate, plus a data access band that the public record does not resolve.

04 The finding

The Australian Commonwealth has placed a concentrated dependence on a single United States controlled software vendor, and that dependence creates foreign exposure of more than one kind. Between 13 May 2023 and 13 May 2026, 22 agencies contracted approximately AUD 694.7 million in VMware products through entities wholly owned by Broadcom Inc, a Delaware corporation. The exposure this creates is not a single thing, and treating it as one obscures both what is at risk and how likely each risk is. Three distinct categories are present.

The first is data access exposure: whether United States legal process could compel disclosure of Commonwealth data through these contracts. This is the exposure most often assumed and it is the most conditional. The CLOUD Act reaches data in the possession, custody, or control of a covered communications or computing service provider. Whether it reaches data under any given VMware contract depends on whether VMware is acting as such a provider and holds the data at all, which turns on deployment: for hosted services where VMware operates the environment, reach is plausible; for licensed software an agency runs on its own systems, holding its own data, it is doubtful. The procurement record does not disclose which describes each contract. Whether this exposure is real for any given contract is therefore genuinely unsettled, and resolving it requires a legal and technical assessment that no framework requires anyone to perform.

The second is supply continuity exposure: whether the United States could compel Broadcom to withhold, degrade, or terminate the supply of these products to an Australian agency. This exposure does not depend on the data questions above and is the most firmly grounded of the three. United States export control and sanctions law applies to US controlled vendors and their foreign subsidiaries, and authorises the government to restrict what they may supply and to whom. A Commonwealth agency dependent on a US controlled vendor for critical infrastructure software is, in consequence, exposed to the possibility that the vendor could be directed by its home government to restrict, degrade, or cease supply. The legal mechanism for such a direction is firmly established; whether it would be exercised against the supply of enterprise software to an allied government's civilian agencies is a separate question of likelihood that this assessment does not resolve. What the assessment establishes is the standing capacity, not its probability of use (ANALYSIS B).

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

The third is corporate control exposure: the United States government's demonstrated willingness to assert national security jurisdiction over Broadcom's proposed Qualcomm acquisition. Broadcom completed its move to a United States parent in 2018, in the same period as its CFIUS reviewed acquisition of Brocade Communications Systems (CLAIM C); and in the same period the United States, following CFIUS review, prohibited Broadcom's proposed acquisition of Qualcomm by Presidential order (CLAIM M). This does not by itself reach Commonwealth data, but it establishes that Broadcom's transactions are subject to US national security review (ANALYSIS B), which conditions the other two exposures.

The Information Security Manual and the Information Security Registered Assessors Program assess security controls. They assess none of these three categories. Whichever exposure one examines, the result is the same in the way that matters: it is assessable, and no framework requires anyone to assess it. The three categories differ in character, one is a conditional data access risk that turns on deployment, one is a firmly established supply continuity capacity of unresolved likelihood, one is a demonstrated pattern of corporate control oversight, but all three are assessable, and none is assessed. That is the gap.

05 Worked examples

Three contracts from the dataset illustrate how the exposure operates in practice, and how much the procurement record itself permits one to say. Each is drawn from the 113 Contract Notices that constitute the source basis. The three differ in what their own AusTender records disclose, and that variation is part of the finding.

1. Australian Taxation Office, CA Mainframe and VMware software licences

Contract Notice CN4142919-A1 (executed 21 March 2025; amendment published 18 December 2025). Value: AUD 108,680,410.66. Supplier: VMware International Unlimited Company (Ireland). The AusTender category is "Software" without further descriptive content, and the contract covers licences for CA Mainframe and VMware products over a three year term (23 March 2025 to 22 March 2028).

Data access exposure here is doubtful on the face of the record. The contract is described as licences for software, which points toward software the agency runs on its own systems, holding its own data, the deployment under which the CLOUD Act precondition of provider possession or control is least likely to be met. The record does not conclusively establish the deployment, so this is not certain, but nothing in the record supports asserting data access reach, and the licence framing points the other way.

Supply continuity exposure is real and is the firmest exposure on this contract. A three year licence dependent on ongoing patches, security updates, and vendor support is exactly the kind of arrangement that United States export control and sanctions reach over a US controlled vendor can interrupt.

Corporate control exposure is real. The supplier is the Irish subsidiary; Broadcom is the Delaware parent; CFIUS jurisdiction over Broadcom establishes United States governmental reach over the corporate vehicle through which the subsidiary contracts with the ATO.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

The contract shows that exposure is not confined to cloud services. It extends to licence relationships, but through the supply continuity and corporate control categories, not necessarily through data access.

2. Australian Federal Police, Provision of software as a service

Contract Notice CN4126523-A1 (executed 25 January 2025; amendment published 24 April 2026). Value: AUD 15,858,443.10. Supplier: VMware Australia Pty Ltd (NSW). AusTender category: "Software as a Service (SaaS - Cloud)".

This is the dataset's strongest data access case, and it is strongest because the record itself discloses the deployment. The contract is categorised as Software as a Service, Cloud, which describes an arrangement in which the vendor operates the environment and holds or processes the customer's data. That is the deployment under which the CLOUD Act precondition of provider possession or control is most likely to be met. Whether reach in fact attaches still depends on operational specifics the record does not contain, so the conclusion remains conditional; but unlike the other examples, the record here points toward, rather than away from, data access exposure.

Supply continuity exposure applies here as elsewhere: the export control and sanctions reach over the vendor extends to a hosted service it operates, so the service could be directed to terminate or degrade. As above, this is a standing legal capacity rather than a prediction that it will be exercised.

Corporate control exposure is real, through Broadcom's parent relationship and CFIUS jurisdiction.

This contract is where the architecture developed in the Telstra assessment (AOS-TEL-2026-001) is most directly comparable, but the comparison also marks a limit. Telstra's strongest data access cases involved cloud services that demonstrably hold customer data. Where a VMware contract is a genuine hosted service, as this one is recorded to be, the same reasoning applies; where it is licensed software, as in Example 1, it does not. The deployment model, not the corporate structure, is what determines whether data access exposure attaches.

3. Australian Signals Directorate, Software Subscription

Contract Notice CN4157511, published 12 June 2025. Value: AUD 36,130,383.04. Supplier: VMware Australia Pty Ltd (NSW). AusTender category: "Software". Title: "Software Subscription".

ASD is the parent agency of the Australian Cyber Security Centre, which produces the Information Security Manual and administers the Information Security Registered Assessors Program. ASD is a customer of the same Broadcom controlled VMware estate, and the ISM and IRAP, by their documented scope, assess security controls rather than the legal authority a vendor's home jurisdiction holds over the vendor. This is an observation about the scope of the frameworks, not a critique of ASD. What ASD does within its own classified arrangements sits outside the public record and outside this assessment. The point is structural: this category of exposure falls outside what the baseline is designed to measure, and that scope limit holds even for the agency that produces the baseline (ANALYSIS D).

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

Data access exposure here is undetermined on the record. The contract is titled "Software Subscription", and a subscription may be either a hosted service the vendor operates or software licensed on a subscription basis that the agency runs itself. The record does not disclose which. Unlike the ATO contract, it does not point away from data access; unlike the AFP contract, it does not point toward it. It simply does not say, which is itself the point.

Supply continuity exposure is real. ASD is dependent on continued vendor service across the subscription term.

Corporate control exposure is real, through the Broadcom parent relationship and CFIUS jurisdiction.

Summary

The three contracts show three different things the procurement record permits one to say about data access exposure. The AFP contract, recorded as Software as a Service, points toward it. The ATO contract, recorded as software licences, points away from it. The ASD contract, recorded only as a software subscription, does not disclose enough to say either way. In all three, supply continuity exposure and corporate control exposure attach, because neither depends on deployment. The variation across the three is not a variation in the underlying corporate structure, which is identical: each is a Broadcom controlled entity holding a Commonwealth contract. It is a variation in what the public record discloses about deployment, and therefore in how much of the exposure can be assessed at all from the record. No framework requires that the record disclose more, and no framework requires anyone to assess what it does disclose.

06 Methodology and limits

Source basis

The assessment used three categories of primary sources. Commonwealth procurement records were extracted from AusTender Contract Notices with supplier name "VMware" for the three year period ending 13 May 2026. Corporate structure was established through SEC filings (Broadcom Inc 10-K and Exhibit 21.1 list of subsidiaries, Form 425 confirming the 2018 CFIUS conditioned redomiciliation), the Irish Companies Registration Office, the Australian Modern Slavery Register, and the Australian Business Register. Legal mechanism analysis drew on US statutes (18 USC 2713, the CLOUD Act 2018, the Export Administration Regulations, and the Foreign Investment Risk Review Modernization Act). The same primary source verification standard applied in AOS-TEL-2026-001 was applied here.

Verification

Every factual claim in this assessment is traceable to a public primary source, and the contract dataset is reproducible. The dataset was extracted on 13 May 2026 by searching AusTender Contract Notices for supplier name containing "VMware", with a publish date range of 13 May 2023 to 13 May 2026. That search returns the 113

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

contract notices analysed here, of which 112 match the extracted dataset exactly.[1] A reader running the same search can reproduce the dataset. AusTender figures are point in time; a contract amended after extraction returns an updated value, and the figures here are stated as at 13 May 2026 accordingly.

The search applies AusTender's own supplier name matching, which is a permissive substring match: it returns every contract notice whose supplier field contains "VMware". This includes both the supplier entities and the single training membership with a United States user community, which is included in the contract figures but excluded from the corporate chain analysis. The full list of the 113 notices, with their identifiers and values, is provided in the contract appendix accompanying this assessment, so that any individual claim can be confirmed against its source. Verification verdicts were assigned using the AustraliaOS verification workflow, and gaps in the source basis were flagged inline rather than papered over.

What this assessment does not claim

This assessment does not predict that specific US legal mechanisms will be used against specific Australian agencies. It does not assess Broadcom intent or future conduct. It does not provide legal advice on Section 2713 or other statutory application to specific data flows. It is not a substitute for individual agency risk assessment. It is not a directive to any agency, vendor, or oversight body.

Limits

Four limits should be noted by any reader applying this analysis.

Contract descriptions on AusTender are sometimes generic. Of the 113 contracts in the source basis, 51 contracts totalling approximately AUD 475 million fall into the generic class, meaning their AusTender titles did not match any of the classifier's descriptive patterns. Of these, 35 contracts totalling approximately AUD 330 million carry literally generic titles such as "Software" or "Licences"; the remainder are generic in the broader sense that no title pattern resolved their deployment. These contracts were individually confirmed as VMware by direct inspection of the public AusTender supplier records; the category classification is based on contract title content. A reader seeking certainty about specific contract content should refer to the originating agency.

Contract values reflect reported AusTender notice values. The corpus contains five amendment Contract Notices, identifiable by an -A amendment suffix on the CN ID (CN4126523-A1, CN4181473-A1, CN4142919-A1, CN4071834-A1, CN4043478-A1). The aggregate AUD 694,715,987 figure was checked for double counting against these: for each of the five, the corresponding base notice does not appear as a separate row in the extracted dataset, because the AusTender export returned only the latest version of each amended contract. The realised double count between original notices and amendments is therefore zero across the five amendments

[1] One contract diverges between the extracted dataset and the live record. CN4204273 appears in the dataset at its base value of $50,500; the live record shows an amendment (CN4204273-A1, published 26 November 2025) bringing the value to $54,396, a difference of approximately $3,900. The amendment predates the extraction date; why it was not captured in the extraction is not established. The effect on the headline figure falls within the rounding of the stated approximate total.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

identified. The published AusTender record does not, in general, disclose per amendment how much of an amended value supersedes versus adds to its base notice; that limit is noted here even though, for the five amendments in this corpus, no base notice duplication is present to resolve. The dataset was further checked against the live record at extraction time: one base notice (CN4204273) was found to have an uncaptured later amendment, documented in the verification footnote.

Corporate structures change. The Broadcom corporate chain documented in section 01 is current as of assessment date. Primary source verification was conducted in May 2026.

The legal mechanism analysis is current as of May 2026. US law changes, US enforcement priorities change, and the Australia-United States CLOUD Act Agreement framework is itself subject to ongoing negotiation.

Review value

The assessment is reviewable. Every claim is traceable to a public primary source. The methodology is documented. The limits are stated.

The reviewing audience is the Commonwealth agencies that hold the relationships, the oversight bodies that have authority over those agencies, and the practitioner and policy community that engages with structural exposure as an analytical category. Final decisions on vendor selection and operational use remain with the agencies that hold the relationships. This assessment produces an analytical position, not a substitute for institutional governance.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002

About AustraliaOS

AustraliaOS Pty Ltd (ABN 69 697 049 291) is a Melbourne based company building decision infrastructure for Australian institutions. The company is owned and directed by Brunel Al-Bijwaie.

The thesis of AustraliaOS is that institutional procurement and risk decisions in Australia must account for exposures that existing assessment frameworks were not designed to measure. Structural exposure to foreign legal jurisdiction is the first such class addressed by the published methodology. Further classes will be addressed in subsequent assessments as the practice matures.

AustraliaOS publishes assessments as methodology demonstrations and offers paid engagements to institutional buyers to support vendor selection, procurement defence, and exit planning.

AustraliaOS carries professional indemnity and public liability insurance through DUAL Australia.

AustraliaOS publishes its own infrastructure dependencies. Several components of the current stack sit under US jurisdiction (model inference, source code hosting, web compute, and persistent storage). Phase 2 commitments and current status are published at australiaos.com.au/#sovereignty-posture. AustraliaOS applies the same standard of jurisdictional honesty to itself that it applies to the vendors it assesses.

Third-party names and marks are the property of their respective owners. AustraliaOS is not affiliated with, authorised by, or endorsed by Broadcom Inc, VMware, or any vendor named.

Engagement enquiries: contact@australiaos.com.au

End of document.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director. · Verification: australiaos.com.au/verify/AOS-BCM-2026-002