What the Instruments Require

REFERENCE	AOS-ASR-2026-001
VERSION	1.5
DATE	23 September 2026
CLASSIFICATION	Released
DIRECTOR	Brunel Al-Bijwaie

Version 1.5, 23 September 2026. This assessment examines eight published Australian assurance instruments and one overseas comparator. It rests entirely on those documents' own text. **Quotations reproduce the source's typography, including its spelling of "cybersecurity" where it prints it that way.** Vocabulary counts state the artefact they were taken from and the control word run on the same extraction.

Version note

This is v1.5, published 23 September 2026. It corrects the first half of the finding, which was false as written for one of the eight instruments from v1.0. **The second half, that none of the eight specifies a method for assessing foreign legal reach, does not change. No other finding, no figure and no quotation of any instrument moves.**

Where	What changed	Why
Section 8, the finding; **Section 2**, its opening sentence; the v1.1 note carried forward below	*"each names or asserts foreign legal reach"* becomes: **none of the eight specifies a method for assessing foreign legal reach, and at least one, the Commonwealth Procurement Rules, does not name it at all**	**This assessment's own text excepts the Procurement Rules.** Section 2 states "The Commonwealth Procurement Rules [`L-CPR-1`] do not name it." and Section 8 states "One does not name it [`L-CPR-1`]." The universal was false as written for that instrument from v1.0
Section 8, the breakdown	Its lead-in no longer repeats *"names or asserts"* as a property of all eight. **The breakdown itself is unchanged**: four state reach in terms, one imposes conditions on ownership and control without naming legal reach, two reach the subject only through a coverage requirement about location, one does not name it	The breakdown is this assessment's own classification, and it is kept as that

Wrong when made, and recorded. The error is entered in this practice's corrections register, in the entry for this assessment dated 23 September 2026, and in its open-items record at item 194. **The finding's second half stays subject to a rule this practice has not decided**, recorded at item 181: whether a method reached by referral is one the instrument specifies. v1.5 does not decide it.

v1.0 to v1.4 remain published at their own addresses with their own hashes.

This is v1.4, published 24 August 2026. It adds two things that were in the Deed of Certification when v1.3 read it and were not reported. **Recommendation F stands. No finding moves, no figure changes, no quotation of any instrument changes, and nothing v1.3 said becomes false.**

Where	What changed	Why
Section 5A	Clauses **13.3, 13.4 and 13.5.1**, and the published **Declaration by Provider** [`A-DEED-2`] at clauses 2(b), 2(c) and 2(d)	**The declaration implementing 13.2's warranty is available at *best endeavours* where 13.3.2 says *will ensure*, and the published form takes the softer standard.** The form reaches a parent company in its awareness limb only, and **carries one signature block**
Section 5A	That *"ultimate parent company"* occurs **once in the whole Deed**, in 13.4, and that all five limbs of `Relevant Change` attach to the Service Provider or the Service	**Read at the passage where a parent obligation would sit**, not inferred from a count — convention 34
Section 5A	The **protective marking** on both documents, counted, with the Framework's own definitions of a security classification and of an information management marker [`AT-PSPF-1`]	**An observation about the record, not a finding about anyone.** It is written that way and its limits are stated
Source register	**`A-DEED-2` appended** as an inherited capture under convention 7, and the register pin moves with it	Nothing added to Section 5A rests on an unpinned source

Addition, not correction, and the test is stated. The corpus's corrections register records a correction where a published document made a statement that is false, and uses a separate heading where a surface changed with none. **v1.3 §5A says the Deed warrants against a change in ownership, defers the assessment method, permits the Authority to determine a change is not one, and defines the only law it will excuse a non-disclosure for as Australian. Clause 13.4 falsifies none of that**, and no published document in this corpus said anything about how the Deed is marked. **Both are additions**, and both are entered in `CORRECTIONS-REGISTER.md` under that heading.

A working record was corrected, and no published document reissues for it. `DEED-RULE-15-AUDIT-2026-08-24.md` cited clause 13.2 at a page that was neither its printed page nor its PDF page, cited a quotation at the page before the one carrying it, and wrote all twelve citations in a numbering it never stated — convention 21. **Every quotation was re-read against its page image and none moves.** This document cites the audit by name and reproduces no Deed page number, so **its text is unaffected.**

This is v1.3, published 24 August 2026. It adds a fourth instrument at the passage where the method would sit, and corrects a scope statement. **Recommendation F stands. No finding moves, no figure changes, and no quotation of any instrument changes.**

Where	What changed	Why
Section 1, the scope list	"the Hosting Certification Framework's ownership and control provisions" becomes **the Framework's published framework document [`AT-HCF-2`]**, and a new line records the **Deed of Certification [`A-DEED-1`]** as read at v1.3	**v1.2 read the framework document, not the Deed in which those provisions operate.** The Deed is published on the framework's own site and linked from no page on it, so it was not reached
Section 5A, new	The Deed at the passage where the method would sit, with its clauses quoted	It is the operative instrument for the Strategic tier's ownership condition and it states no method. **The finding gains an instrument**
Source register	**`A-DEED-1` appended**, and the register pin moves with it	Nothing in Section 5A rests on an unpinned source

Why the addition sharpens rather than qualifies. v1.2 found that no instrument specifies a method for assessing foreign legal reach. The Deed warrants against a change in ownership, defers the assessment method to whatever the Certifying Authority notifies, permits that Authority to determine that a change is not a Relevant Change at all, and **defines the only law it will excuse a non-disclosure for as Australian**. **An absence established by a definition is stronger than one established by a control-word count**, and Section 5A says so in those terms.

How it was found. By re-testing, on 24 August 2026, whether the Deed was obtainable at all — a statement three published documents made and this one did not. **It was obtainable, and had been since November 2021.**

This is v1.2, published 20 August 2026. It corrects three defects, **none of which touches a finding.** All three sit in the apparatus that lets a reader check the findings: a quotation truncated mid-sentence, a statement about what was retrieved that no pinned artefact evidenced, and a classification with no artefact behind it.

Where	What changed	Why
Section 5, the PSPF referral	The quotation is **restored to the full sentence**, adding the circular's subtitle and "(on GovTEAMS)"	It was introduced as "the sentence" and stopped mid-sentence with no ellipsis. **The subtitle names physical security certification of facilities**, which bears on the assessment's own reliance on that referral, so its omission engaged convention 20
Section 1 and Section LM, the landing pages	v1.0 and v1.1 said landing pages "were retrieved" for two NIST catalogues and the CSA matrix. **No register row, hash, path or retrieval time evidenced it.** The three are now **retrieved and pinned at this revision** [G-NIST-2, G-NIST-3, G-CSA-1], and the sentences say what is pinned	**Retrieving them today does not make the earlier sentence true.** Whether a retrieval happened in early August is not established and is not now establishable. The earlier assertion is recorded as unevidenced rather than repeated
Section 6, the referral table	NIST SP 800-145 now carries a reference [G-NIST-1]	It was classified **Public** with no reference and no register row, while both **not obtainable** rows carried their method. **Tested 20 August 2026: HTTP 200, 85,781 bytes, 7 pages.** The classification holds and **the count of six referrals — three public, two to one unobtainable document, one not followed — does not move**

No finding moves, no claim moves, and no quotation in v1.0 or v1.1 is withdrawn or qualified. One

quotation is **lengthened** to the source's own full stop.

The earlier correction, carried forward. v1.1 corrected one figure and one limitation from v1.0 of the same day.

Where	What changed at v1.1	Why
Section 1, the domain statement	"Not read: **ten** further cloud publications listed on the ASD cloud computing page" is replaced. **The page lists eight publications, one examined and seven read at this revision**	The count was wrong when published. Counted from `G-ASD-3` two ways at this revision — `<h3>` headings and card hyperlinks — both returning eight, and the live page the same day also returns eight
The `G-ASD-3` register row	"lists **eleven** cloud publications" becomes **eight**	Same figure, same cause

Where the error came from. The count was taken from reading the page's prose and never recomputed against it. It was carried into the register row when the artefact was pinned, and from the row into Section 1.

What the seven establish, and what they do not. None specifies a method for assessing foreign legal reach. **The finding is unchanged**: none of the eight named Australian assurance instruments specifies a method for assessing foreign legal reach. (Corrected at v1.5: this sentence also read *each name or assert*, which the Procurement Rules do not.) **No hub publication is one of the eight**, and the hub is cited for one thing — that the Common Assessment Framework's footnote resolves to a page listing publications rather than to a document.

v1.0 and v1.1 both remain published at their own addresses with their own hashes, and all three versions resolve.

1. Scope

This assessment puts one question to eight instruments:

Where an instrument names or asserts that a foreign government may reach a provider's data by law, does it specify a method for assessing that reach?

The eight, each pinned and read:

Instrument	Ref
ASD, *Cloud assessment and authorisation*, January 2024	`G-ASD-1`
ISM, *Guidelines for procurement and outsourcing*, June 2026	`I-ISM-2`
Protective Security Policy Framework, Release 2025	`AT-PSPF-1`
PSPF Direction 001-2024	`L-PSPF-1`
Hosting Certification Framework, March 2021 v2	`AT-HCF-2`
Commonwealth Procurement Rules 2025	`L-CPR-1`
ASD, IRAP Policy and Procedures v2.0	`IR-ASD-1`
ASD, IRAP Common Assessment Framework	`IR-ASD-8`

The comparator, read for one purpose only: UK NCSC, *Cloud security principle 2* [`G-UK-1`].

"Method" means, throughout: a stated test, a stated source, or a stated standard of evidence by which an assessor would establish who can compel a provider. An instrument that names the question, or requires that it be considered, has not thereby specified a method. **This definition is stated before the finding rather than after it, because the finding turns on it.**

The domain, stated before the finding.

- **Read in full:** the ISM procurement chapter; PSPF Direction 001-2024; the ASD *Cloud assessment and authorisation* section on provider locality and ownership; IRAP-AR-0019 and its summary-table restatement; UK NCSC principle 2.1.
- **Read in part, at the passage where the method would sit:** PSPF Release 2025 §15.2.3; **the Hosting Certification Framework's published framework document [`AT-HCF-2`]** at its ownership and control provisions; the Commonwealth Procurement Rules; IRAP Policy and Procedures §1.3.2 and §4.1.1.
- **Read at v1.3, and not read before it:** the **Deed of Certification [`A-DEED-1`]**, the instrument in which those ownership and control conditions operate. **v1.2 named "the Hosting Certification Framework's ownership and control provisions" and read the framework document, not the**

Deed that carries them. The Deed was reached on 24 August 2026 and read at page-image resolution. **It confirms the finding, and Section 5A states how.**

- **Read at v1.4:** the **Declaration by Provider [A-DEED-2]**, the published form of the declaration clauses 13.3 and 13.4 provide for, **and the Deed re-read in full at clauses 13.3 to 13.5. v1.3 read the Deed and reported part of clause 13.** Both documents were read again at page-image resolution on 24 August 2026.
- **Read at this revision:** the ASD cloud computing page [G-ASD-3] lists eight publications. One, *Cloud assessment and authorisation*, is examined above. **The other seven were read on 19 August 2026 and none specifies a method for assessing foreign legal reach.** The closest of the seven is *Cloud computing security for cloud service providers*, whose mitigation table asks a provider to "Disclose the countries and legal jurisdictions where tenant data is (or will be in the coming months) stored, backed up, processed and accessed by CSP staff for troubleshooting, remote administration and customer support" — **a disclosure obligation about location, not a test for who can compel.** The word *extrajudicial* does not appear in any of the seven.
- **Not read:** the Defence Industry Security Program; Digital Transformation Agency cloud guidance; ISO 27001, 27002, 27036 and 31000, which are paywalled; and the control catalogues of NIST SP 800-53 and SP 800-161 and of the Cloud Security Alliance, of which only the publication landing pages are held [G-NIST-2, G-NIST-3, G-CSA-1].

This assessment makes no finding about any agency, provider, assessor or system. Section LM sets out what it does not say.

2. What the instruments name

Four of the eight name foreign legal reach in terms, and at least one, the Commonwealth Procurement Rules, does not name it at all.

The ISM procurement chapter [I-ISM-2], printed p 1:

> "foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers."

The Protective Security Policy Framework, Release 2025, §15.2.3 [AT-PSPF-1], printed p 79:

> "Foreign-owned service providers may be subject to extrajudicial control and interference by a foreign entity. This could include a foreign entity compelling a service provider to disclose its customers' data unbeknownst to its customers."

PSPF Direction 001-2024 [L-PSPF-1], printed p 1:

> "Foreign Ownership, Control or Influence (FOCI) is an application of foreign interference."

ASD, *Cloud assessment and authorisation* [G-ASD-1], printed p 7:

> "This could include a foreign entity compelling a CSP to disclose its customers' data unbe-

> knownst to its customers. This can include foreign-owned CSPs that provide cloud services in and from Australia."

The Hosting Certification Framework [`AT-HCF-2`] names ownership and control rather than legal reach, imposing conditions where a provider "does not have ultimate control or ownership over the core capabilities underpinning the services it is providing".

The Commonwealth Procurement Rules [`L-CPR-1`] do not name it. Test: `jurisdiction` returns zero across 85,269 characters of extracted text on which the control word `procurement` returns 336. The single occurrence of `compel` concerns compatibility of equipment on a change of supplier and is not on this subject.

3. The closest instrument, and what it does and does not do

ASD's *Cloud assessment and authorisation* [`G-ASD-1`] comes closer than any other instrument read, and this section states what it does before stating what it does not.

It names the factors, in a list, quoted in full, printed p 7:

> "Cloud consumers, as part of their review of a CSP, need to consider the following: the ownership of the CSP · the locality of the CSP's offices, datacentres and administrative and support personnel · whether the CSP's personnel are employed by the CSP or a subcontracted · where its cloud services are provided from · the potential for any extrajudicial control and interference over a CSP by a foreign entity."

It separates ownership from location, and location from operation:

> "CSPs that are owned, based and solely operated in Australia are more likely to align to Australian standards and legal obligations."

And it states, expressly, that being in Australia does not settle the question:

> "This can include foreign-owned CSPs that provide cloud services in and from Australia."

What it does not do. It states what to consider. **It states no test by which ownership is established, no source from which locality is read, and no standard of evidence for concluding that a provider is or is not subject to extrajudicial control.** The passage where such a test would sit is the five-item list quoted above; it was read in full, and the list is what is there.

Its status is guidance. It uses "ASD recommends", "need to consider" and "ASD considers that". **The document nowhere states what an assessor may not conclude.**

Vocabulary, whole document, control word `cloud` = 460 on the same extraction: `jurisdiction` zero, `compel` one, `foreign` fifteen, `ownership` seven.

4. What the other instruments specify

The ISM procurement chapter. The chapter carries **thirty-eight controls**. **Test:** every `ISM—<number>` identifier in the extracted text of the chapter, counted on 19 August 2026 across four extractions — `pdftotext` with no flag, with `-layout`, with `-raw`, and PyMuPDF — each returning thirty-eight distinct identifiers and thirty-eight occurrences of the printed string `Control:`, with no identifier appearing outside a control line. **The assertion quoted in Section 2 sits in the chapter's opening narrative, and no control in the chapter names jurisdiction, foreign ownership, offshore location or sovereignty.** The passage where such a control would sit is the chapter's control set, which was list-read in full. `jurisdictional` occurs twice, both in a single paragraph of the opening narrative; `compel` occurs zero times, on an extraction where `control` returns 40.

PSPF Release 2025 §15.2.3. It requires that the matter be considered — "These arrangements need to be considered as part the entity's assessment to determine if the service provider is suitable for handling its data" — and the sentence that follows the assertion is a referral: "See Australian Signals Directorate's Cloud Assessment and Authorisation and ASIO's Protective Security Circular 149— Physical security certification of outsourced information and communications technology facilities (on GovTEAMS)". **The passage where a method would sit is that referral**, and the referral's own subtitle names a subject — physical security certification of facilities — that is not the assessment of who can compel a provider.

PSPF Direction 001-2024. It requires entities to "implement a process when undertaking procurement of technology assets to identify and manage potential FOCI risks", "in accordance with Department of Home Affairs guidance". **The requirement names no document in that sentence, and the Direction states no test.** On an extraction where the control word `FOCI` returns 6 across 3,650 characters, `jurisdiction`, `compel`, `legal` and `evidence` each return zero.

The Hosting Certification Framework. Its ownership and control provisions state what conditions attach to certification. **They state no method for establishing foreign legal reach.** Control word `certification` = 104 across 58,244 characters; `jurisdiction` and `compel` each return zero, `foreign` returns nineteen and `ownership` forty.

5. The mandatory methodology, and what its coverage requirement asks

IRAP Policy and Procedures v2.0 [`IR-ASD-1`] defers the method, at §4.1.1, printed p 14:

> "All IRAP assessments are expected to uphold the high standards of the program and follow the methodologies outlined in the IRAP Common Assessment Framework."

The scope of an IRAP assessment, at §1.3.2:

> "An IRAP assessment includes determining the effectiveness of relevant security controls outlined within the Information Security Manual (ISM)."

The Common Assessment Framework [`IR-ASD-8`] carries one requirement in this territory, quoted in full:

IRAP-AR-0019, printed under the heading `Coverage` and dated `Apr 2025`, at printed p 19:

> "The IRAP assessment report covers aspects regarding data sovereignty, offshore equipment and staff, or any information (including metadata) that is not within Australia."

The requirement has three limbs and each is a question about where something is: data sovereignty; offshore equipment and staff; information not within Australia. **The requirement does not ask who could compel the provider.**

This is a coverage requirement and it is mandatory, because §4.1.1 makes the framework the methodology. **An assessor who reports on all three limbs has met it.**

Vocabulary. In IRAP Policy and Procedures, on an extraction where `IRAP` returns 587 and `assessor` returns 182 across 74,240 characters: `jurisdiction`, `foreign`, `compel`, `offshore`, `sovereign` and `FOCI` each return zero. **In the Common Assessment Framework, on an extraction where `assessment` returns 361 and `system` returns 128 across 92,205 characters:** `jurisdiction`, `foreign`, `compel` and `ownership` each return zero; `offshore` returns two and `sovereign` returns two, **and both pairs fall inside IRAP-AR-0019 and its restatement in the document's summary table.**

5A. The Deed of Certification, added at v1.3

The Framework's ownership and control conditions do not operate in the framework document. They operate in a Deed, and the Deed is published: `A-DEED-1`, *Deed of Certification (Template)*, 20 pages, on the framework's own site and linked from no page on it. **v1.2 read the framework document at this passage and not the Deed.** Read at page-image resolution on 24 August 2026; audit at `DEED-RULE-15-AUDIT-2026-08-24.md`.

It is the fourth instrument at the passage where the method would sit, and like the other three it states no method. What it states instead is sharper.

It is the operative instrument. Recital A: the Framework *"is intended to assist Commonwealth Entities to mitigate against supply chain and Service Provider ownership and control risks."* Clause 13.2 carries the condition:

> "The Service Provider confirms and warrants that for the term of the Deed (and any Contract) there will be no Relevant Change except as agreed by the Certifying Authority."

`Relevant Change` reaches ownership, at limb (b):

> "a significant change in strategic direction or ownership of the Service Provider that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the Service Provider's Services to Commonwealth Entities"

No test is stated for any of it. `Assessment` is defined as *"the process the Service Provider must comply with... **as notified by the Certifying Authority from time to time**. The Assessment may be included in an Information Security Registered Assessors Program assessment or may be a different process."* **The instrument**

defers the method to notification, and IRAP is named as one thing it *may* be.

And the Certifying Authority may remove the question. Clause 13.7:

> "If the Certifying Authority confirms that a change is not considered a Relevant Change, then it will not be a Relevant Change for the purpose of this Deed."

Nothing in the Deed states how it decides.

And the declaration that carries the warranty is available at a lower standard than the clause that requires it. Clause 13.3 requires a declaration, on the Deed Effective Date and within 30 days of each anniversary, that the Service Provider *"13.3.2 will ensure that a Relevant Change does not occur, except as agreed by the Certifying Authority."* Clause 13.4:

> "The Service Provider may provide a single annual declaration from the Service Provider (and where applicable, its ultimate parent company's directors and relevant officers/Board members) that they are aware of the above requirements and that they will use their **best endeavours** to ensure that the events and circumstances specified as a Relevant Change do not occur."

`Will ensure` and `best endeavours` are not the same undertaking, and the Deed offers both.

It is an alternative form of the same declaration rather than a second obligation — 13.4 is permissive and consolidating, and clause 13.5.1 refers to *"providing its annual declaration (as set out in clauses 13.3 and 13.4)"*, one declaration described across two clauses. **The Deed does not say "in lieu of"**, and 13.3's Deed Effective Date declaration is not annual, so the narrow reading is that **13.4 governs the recurring declaration's form and its parties, and 13.3 governs its timing and content.** This assessment takes the point no further than that.

The published form settles which standard is used, and it takes the softer one. `A-DEED-2`, *Declaration by Provider*, is the form the Certifying Authority publishes. Its operative warranty is clause 2(d):

> "[The Service Provider] warrants that it will use its best endeavours to ensure that a Relevant Change does not occur, except as agreed by the Certifying Authority and/or the relevant Agency."

The form takes 13.4's standard without taking 13.4's parties. A parent appears only at clause 2(b), where the provider *"confirms that it (including its directors, relevant officers, Board members, and any applicable ultimate holding company) is: (i) aware of; and (ii) understands"* the requirements — **an awareness limb, not a warranty.** The warranties at 2(c) and 2(d) are the provider's alone, and **the form carries a single signature block**: one signatory, one witness, and **nowhere for a parent company officer to sign.**

No other clause reaches a parent. *"Ultimate parent company"* occurs **exactly once in the Deed** — in clause 13.4 — and *"holding company"* not at all. Read at the passage where such an obligation would sit: **all five limbs of `Relevant Change` attach to the Service Provider or to the Service.** Limb (b) reaches *"ownership of the Service Provider"*, so a transaction at parent level that changes who owns the provider is caught — **but the obligation holder remains the provider, and the standard available to it is best endeavours.**

How the Deed and its form are marked, and what is not claimed by saying so. Both documents carry *"Official: Sensitive Legal - Privilege"* in the header and the footer of **every page — 22 pages, 44 occurrences, none without it.** `OFFICIAL: Sensitive` is a security classification: the Protective Security Policy Framework [`AT-PSPF-1`] states that *"the Australian Government uses four security classifications: OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET"*, and places it at business impact level 2, expected damage *"Limited damage to an individual, organisation or government generally if compromised."* The second half of the marking is of a different kind — the Framework states that *"information management markers are an optional way for entities to identify information that is subject to non-security related restrictions on access and use... Information management markers are not protective markers or security classifications."* **Neither pinned release of the Framework names this particular marker**, referring the reader instead to guidelines the practice does not hold, so **this assessment establishes what such a marker is and not what this one means.**

This is an observation about the record and not a finding about anybody. Nothing is claimed about whether publication was intended, authorised, or an error; nothing about whether the classification was correctly applied in 2021 or now; nothing about any person. **The observation is only that the marking and the publication say different things**, on a document that has been openly available on a Commonwealth website since November 2021 and held by the Internet Archive since 7 March 2022.

The foreign-reach silence is established by a definition, not by a count, and that is why it is stronger. The Deed's only law-based disclosure carve-out is clause 13.10 — a provider *"is not required to disclose information pursuant to this Deed to the extent that it would cause the Service Provider to breach any* ***Relevant Laws*** *or duty of confidentiality restricting disclosure of the information"*. And `Relevant Laws` is closed by its own parenthesis:

> "**Relevant Laws** means any relevant common law, statute, regulation, by-law, ordinance or subordinate legislation **(whether made by a State, Territory or the Commonwealth)** in force from time to time."

A foreign order is outside that definition as a matter of construction. The carve-out cannot contemplate one, and no other clause supplies it. The instrument's two uses of the word *foreign* both name Australian foreign-**investment** law — *"Another Relevant Framework means the Foreign Acquisitions and Takeovers Act 1975 (Cth), Foreign Acquisitions and Takeovers Regulation 2015 (Cth), or (once legislated) the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth)"* — and its single use of *jurisdiction* is the governing-law clause submitting to the courts of the Australian Capital Territory.

What this adds to the finding, stated at its narrowest. The instrument that carries the Strategic tier's ownership condition warrants against a change in ownership, **offers the declaration implementing that warranty at best endeavours as well as at "will ensure", and reaches a parent company in one permissive clause and nowhere else**, defers the assessment method to notification, permits the Certifying Authority to determine that a change is not one, and **defines the only law it will excuse a non-disclosure for as Australian. Recommendation F stands, and the Deed is a fourth instrument establishing why it is needed rather than a counterexample to it.**

What is not claimed. That the Deed ought to address foreign reach; that any executed Deed omits it; that the Certifying Authority does not assess it in practice; **that best endeavours is the wrong standard, or that any provider has given a declaration in any particular form. Nothing executed is public** — not which providers hold a Deed, not any variation, not any condition imposed under 13.2 or confirmation given under 13.7, **not any declaration made under 13.3 or 13.4, and not whether the Certifying Authority has agreed a different form under the published form's own clause 2(c)** — and this section characterises none of it.

6. Where the instruments send a reader next

Six referrals were followed one step each. The table states what each resolves to.

Referring document	Points to	Resolves to
PSPF Direction 001-2024	Policy Explanatory Note 01/24	Not publicly obtainable
PSPF Release 2025 §15.2.3	ASD, *Cloud assessment and authorisation*	Public [`G-ASD-1`]
PSPF Release 2025 §15.2.3	ASIO T4 Protective Security Circular 149	Not publicly obtainable
ASD *Cloud assessment and authorisation*	ASIO T4 Protective Security Circular 149	Not publicly obtainable
ASD *Cloud assessment and authorisation*	NIST SP 800-145	Public [G-NIST-1]
IRAP Policy and Procedures §4.1.1	IRAP Common Assessment Framework	Public [`IR-ASD-8`]

Six referrals: three resolve to public documents, two to one document that is not publicly obtainable, and one was not followed. The referral not followed is ASD *Cloud assessment and authorisation*'s reference to Department of Home Affairs security requirements and cloud guidance. **Nothing is claimed about it.**

Two referrals name a document as carrying guidance on this subject, and both name a document this practice could not obtain.

PSPF Direction 001-2024:

> "Further information about FOCI as it relates to procurement is detailed in Policy Explanatory Note 01/24 – Managing Foreign Ownership, Control or Influence Risk in technology assets."

ASD, *Cloud assessment and authorisation*:

> "ASIO T4 Protective Security Circular 149 – Physical security certification of outsourced ICT facilities (available to cloud consumers on GovTeams) provides additional guidance on PSPF im-

> plementation in the outsourced ICT facility or data centre environment, including considering the security risks of using foreign-owned providers and storing data offshore."

On 11 August 2026 this practice searched for a publicly retrievable copy of Policy Explanatory Note 01/24 and did not find one. The routes tried were three constructed paths, each returning HTTP 404; the PSPF publications library rendered in a browser, whose complete forty-item catalogue was enumerated across all four pages and whose publication-type taxonomy carries no Explanatory Note category; the Wayback CDX index for three patterns, each returning an empty result set; and a Home Affairs site search, which returned HTTP 401. **This is a statement about what a search on that date found. It is not an assertion that the note does not exist.**

ASIO T4 Protective Security Circular 149 is recorded by the referring document itself as available on GovTeams. This practice did not obtain it.

7. One comparator

UK NCSC, Cloud security principle 2.1, is read for one purpose: to establish that an instrument can draw the distinction expressly. [G-UK-1]

> "You need to identify which legal jurisdiction(s) your data could be subject to, seeking legal advice as necessary. This may be more complex than simply clarifying the physical locations where data is stored, processed, or accessed by the service provider. You should also consider: the legal base of the service provider · locations where the service is supported and operated from · who owns and is responsible for the physical data centre · the governing legislation of any contracts/agreements between you as a user of the service (or their suppliers) and the provider"

It separates legal jurisdiction from physical location in terms. Where a standard of evidence would sit, it says "seeking legal advice as necessary".

One comparator was read. FedRAMP, the European Union's cloud certification scheme, Canada's ITSG and cloud guardrails, and New Zealand's GCSB framework were not reached. Nothing here says that Australia should adopt anything, and nothing here is a verdict on either country's choices.

8. The finding

Across the eight Australian instruments read, none specifies a method for assessing foreign legal reach, and at least one, the Commonwealth Procurement Rules, does not name it at all.

How the eight relate to foreign legal reach, on this assessment's classification. Four state in terms that a foreign government may compel a provider [I-ISM-2, AT-PSPF-1, L-PSPF-1, G-ASD-1]. One imposes conditions on ownership and control without naming legal reach [AT-HCF-2]. Two govern what an assessor does and reach the subject only through a coverage requirement about location [IR-ASD-1, IR-ASD-8]. One does not name it [L-CPR-1].

"Specifies no method" means, in each case, that the passage where a test, a source or a standard of

evidence would sit was read, and none is there. Section 3 records where that passage is in the closest instrument; Sections 4 and 5 record it for the others.

The single mandatory requirement in this territory asks where things are. IRAP-AR-0019 requires coverage of data sovereignty, offshore equipment and staff, and information not within Australia. **All three limbs are questions about location.**

Two of the six referrals name a document as carrying guidance on this subject, and neither of those documents was publicly obtainable to this practice. Three of the six resolve to public documents, and those three carry, respectively, a list of factors without tests, a coverage requirement about location, and a terminology reference.

LM · Limitations of this assessment

These are carried unchanged from the scoping record, where they were written before any finding.

It does not say any assessor has done anything wrong. IRAP-AR-0019 is a mandatory coverage requirement, and an assessor who meets it is meeting what is required.

It does not say any framework should require more. Whether an instrument ought to specify a method is a judgement about policy, and this assessment does not make it, in either direction.

It does not say the unobtainable documents contain nothing. Policy Explanatory Note 01/24 and ASIO T4 Protective Security Circular 149 are **unread**. Both are described by their referring documents as covering this territory. What is established is that this practice could not obtain them on the dates and by the routes stated in Section 6, and nothing whatever about their content.

It asserts no consequence for any agency, provider or system. No claim is made that any data has been accessed, that any provider is subject to any foreign direction, or that any system is exposed.

One comparator jurisdiction was read. Four named jurisdictions were not reached, and no international standard body's control catalogue was read: ISO 27001, 27002, 27036 and 31000 are paywalled and unread, and for NIST SP 800-53 and SP 800-161 and the Cloud Security Alliance's Cloud Controls Matrix **only the publication landing pages are pinned** [G-NIST-2, G-NIST-3, G-CSA-1], retrieved at this revision; **neither catalogue was read.** Versions 1.0 and 1.1 stated that landing pages had been retrieved and pinned no artefact evidencing it; that assertion is not repeated.

The referral chain is six pointers. It is not a claim about referrals in general, and the counts in Section 6 are the whole of it.

The eight Australian instruments read are those listed in Section 1. The Defence Industry Security Program, Digital Transformation Agency cloud guidance, professional assurance standards and academic frameworks were not reached.

"Specifies" throughout means "states in the document's own text". Several of these instruments are guidance rather than legislative instruments, and nothing here should be read as a statement about legal

obligation.

Related published assessments

AOS-ISM-2026-001 examines one chapter of the Information security manual and asks whether any control requires an organisation to establish whether a supplier is subject to foreign lawful access. **This assessment covers the same ISM chapter as one of eight instruments and reaches it through the same kind of reading.** Where the two documents state the same thing about I-ISM-2, that is because they read the same passage.

AOS-HCE-2026-001 examines section 30AB(4) of the *Security of Critical Infrastructure Act 2018*. **No claim in this assessment traces to it.**

End of document.