What the Instruments Require

REFERENCE	AOS-ASR-2026-001
VERSION	1.0
DATE	19 August 2026
CLASSIFICATION	Released
DIRECTOR	Brunel Al-Bijwaie

Version 1.0, 19 August 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.

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 ownership and control provisions; the Commonwealth Procurement Rules;

IRAP Policy and Procedures §1.3.2 and §4.1.1.

- **Not read:** ten further cloud publications listed on the ASD cloud computing page [G-ASD-3]; the Defence Industry Security Program; Digital Transformation Agency cloud guidance; ISO 27001, 27002, 27036 and 31000, which are paywalled; the control catalogues of NIST SP 800-53 and SP 800-161 and of the Cloud Security Alliance, of which only landing pages were retrieved.

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

Each of the eight names or asserts foreign legal reach, and four do so in terms.

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 unbeknownst 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". **The passage where a method would sit is that referral.**

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.**

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
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 implementation 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, each names or asserts foreign legal reach and none specifies a method for assessing it.

"Names or asserts" is met in different ways. 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 only landing pages were retrieved for NIST SP 800-53 and SP 800-161 and for the Cloud Security Alliance's Cloud Controls Matrix.

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.