

AustraliaOS Pty Ltd

The Jurisdiction Gap

Recommendation F asked for a methodology standard modelled on the existing IRAP and PSPF assurance pathways. Examination of those pathways establishes that they are not a model for this question. A correction, and a fifth supplement.

REFERENCE

DATE

CLASSIFICATION

CORRECTS

AOS-AIDC-2026-001-
SUPP-05October
2026

Public

AOS-AIDC-2026-
001

Contents

Correction at v1.1, 6 October 2026	3
01 Purpose of this supplement	4
02 What the instruments name, and what they specify	5
03 The one mandatory requirement, and what it asks	6
04 Where the instruments send a reader next	7
05 What this changes, and what it does not	8
Appendix A. Sources	9

Correction at v1.1, 6 October 2026

Five statements in v1.0 claimed more than this supplement's own pages support. Part of the first was wrong when this supplement was lodged, the third was wrong for PSPF Release 2025, and the fifth was a miscount. All five are restated. No recommendation changes.

v1.0 said that each of the eight instruments names or asserts foreign legal reach, and that four do so in terms. The first part was wrong when this supplement was lodged: section 02 says the Commonwealth Procurement Rules do not name the question. This supplement's own pages do not support it for four more. Section 02 says the Hosting Certification Framework imposes ownership and control conditions and that *jurisdiction* does not occur in it. The words section 02 quotes from PSPF Direction 001-2024 require a process, when procuring technology assets, for potential foreign ownership, control or influence risks; they name neither a foreign government's access to a provider's data nor a foreign entity compelling a provider to disclose it. Section 03 says that across IRAP Policy and Procedures and the Common Assessment Framework, *jurisdiction*, *foreign* and *compel* do not occur. The second part named no instrument. Read with the four section 02 then quotes, it counted the Direction, and is not supported either. **Section 02 now opens by saying, for each of the eight, only what this supplement's pages and the instruments' own words support.**

v1.0 also said, in section 01, that the Infosec Registered Assessors Program names or asserts that a foreign government may reach a provider's data by law, and, in section 05, that it names that risk. Section 03 says its one requirement in this territory asks where things are, and that it does not ask who could compel the provider. **Sections 01 and 05 now say so.**

v1.0 also said, in section 01, that each of the eight was read at the passage where such a method would sit. PSPF Release 2025 has a second passage of that kind, §6.1.3, and it was not read. **Section 01 now says so.**

v1.0 said, in sections 01 and 05, that the ISM, the PSPF and IRAP supply or specify no method for assessing foreign legal reach, without saying it meant their own text. PSPF Release 2025 §6.1.3 refers to Home Affairs guidance that asks whether a foreign government could compel a vendor, and to an ASIO tool this practice has not obtained. **Section 01 now says this supplement's statements of that kind speak of each instrument's own text, and section 05 records the referrals.**

v1.0 also miscounted its referrals in section 04: it said one was not followed, and all six were. Three resolve to public documents and three to two documents that are not publicly obtainable. **Section 04 now says so.**

The copy lodged with the committee is unchanged and has not been re-lodged. It is v1.0, 1b75815703188e8901952ff7d98a2604b550becd0c2e6342b8bee5aa3e5534d1, and remains downloadable at its own address. The committee secretariat was told on 23 September 2026 that the sentence “Each of the eight names or asserts foreign legal reach.” is wrong as written for the Procurement Rules.

01 Purpose of this supplement

This supplement corrects the premise of a recommendation in the practice’s own original submission. It withdraws no recommendation and adds none. **Recommendation F stands. Its stated model does not.**

The correction is this. Recommendation F of AOS-AIDC-2026-001, lodged in this inquiry, asked the committee to establish a methodology standard for jurisdictional exposure assessment, **“modelled on the existing IRAP and PSPF assurance pathways”**, and told the committee that this is **“the same approach already used in Commonwealth security assurance.”**¹

Examination of those pathways establishes that on this question they are not a model.

The Information Security Manual and the Protective Security Policy Framework each name or assert that a foreign government may reach a provider’s data by law, and the Infosec Registered Assessors Program’s one requirement on the subject asks where data, equipment and staff are. **None of them specifies in its own text a method for assessing that reach** — a stated test, a stated source, or a stated standard of evidence by which an assessor would establish who can compel a provider. **“Supplies” and “specifies” throughout mean “states in the document’s own text”**, and section 05 records the referrals that reach further.

How it was found. Between 15 and 19 August 2026 this practice examined the eight published Australian assurance instruments named in this supplement, reading each at the passage where such a method would sit (in PSPF Release 2025, §15.2.3; its second passage of that kind, §6.1.3, was not read).² The finding is published as AOS-ASR-2026-001 with a verification record.³ **That assessment is cited here as a pointer to the working — the pinned artefacts, the page images, the vocabulary counts. Every claim in this supplement is restated from the instrument itself and is footnoted to that instrument.**

Why it matters to the committee. A recommendation that says *build this, modelled on that* invites the reading that the pathway already exists and needs only extending. **On**

¹AOS-AIDC-2026-001, Recommendation F. See Appendix A, item 1.

²Protective Security Policy Framework, Release 2025, §6.1.3, printed pages 25 to 26. See Appendix A, item 4.

³AOS-ASR-2026-001, sections 1 to 8. See Appendix A, item 2.

this question it does not exist in the instruments named. The committee should not be left to infer otherwise.

02 What the instruments name, and what they specify

Three of the eight name foreign legal reach in their own words: the ISM, PSPF Release 2025 and ASD's *Cloud assessment and authorisation*. The first two are quoted below. ASD's document says, at printed page 7: **"This could include a foreign entity compelling a CSP to disclose its customers' data unbeknownst to its customers."**⁴ PSPF Direction 001-2024 requires a process, when procuring technology assets, to identify and manage potential foreign ownership, control or influence risks. The Hosting Certification Framework imposes ownership and control conditions, IRAP Policy and Procedures and the Common Assessment Framework between them carry one requirement on the subject, which asks where things are, and the Commonwealth Procurement Rules do not name the question.

The ISM's *Guidelines for procurement and outsourcing*, June 2026 release, printed page 1: **"foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers."**⁵

The Protective Security Policy Framework, Release 2025, printed page 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."**⁶

PSPF Direction 001-2024, printed page 1, requires entities, "in accordance with Department of Home Affairs guidance", to **"implement a process when undertaking procurement of technology assets[2] to identify and manage potential FOCI risks, calibrated to the entity's risk environment."** The bracketed numeral is the Direction's own footnote marker, retained here. **The requirement names no document in that sentence**, and the Direction states no test.⁷

The Australian Signals Directorate's *Cloud assessment and authorisation*, January 2024, printed page 7, comes closest of the eight. It gives a list, reproduced here as the document prints it:

"Cloud consumers, as part of their review of a CSP, need to consider the following:

⁴ASD, *Cloud assessment and authorisation*, printed page 7. See Appendix A, item 6.

⁵ISM, *Guidelines for procurement and outsourcing*, June 2026, printed page 1. See Appendix A, item 3.

⁶Protective Security Policy Framework, Release 2025, §15.2.3, printed page 79. See Appendix A, item 4.

⁷PSPF Direction 001-2024, printed page 1, requirement 1. See Appendix A, item 5.

- 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.”⁸

The third item's wording is the document's own. It separates ownership from location and from operation — “**CSPs that are owned, based and solely operated in Australia**” — and states that being in Australia does not settle the question: “**This can include foreign-owned CSPs that provide cloud services in and from Australia.**”⁹

What none of them supplies is a test. The ASD document states what to consider and 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 itself.

The ISM chapter carries 38 controls. The assertion quoted above sits in the chapter's opening narrative, and **no control in the chapter names jurisdiction, foreign ownership, offshore location or sovereignty**. Across the chapter, *jurisdictional* occurs twice, both in a single paragraph of that narrative, and *compel* does not occur.¹⁰

The Hosting Certification Framework imposes ownership and control conditions on core capabilities and states no assessment of legal reach; *jurisdiction* does not occur in it.¹¹

The Commonwealth Procurement Rules do not name the question.¹²

03 The one mandatory requirement, and what it asks

IRAP Policy and Procedures version 2.0, printed page 14, makes the *IRAP Common Assessment Framework* the operative methodology: “**All IRAP assessments are expected to uphold the high standards of the program and follow the methodologies outlined in the IRAP Common Assessment Framework.**”¹³

⁸ASD, *Cloud assessment and authorisation*, printed page 7. See Appendix A, item 6.

⁹ASD, *Cloud assessment and authorisation*, printed page 7. See Appendix A, item 6.

¹⁰ISM, *Guidelines for procurement and outsourcing*, June 2026: 38 controls, counted from every ISM-
<number> identifier in the chapter across four extraction methods on 19 August 2026; *jurisdictional* twice, *compel* zero, on an extraction where the control word *control* returns 40. See Appendix A, item 3.

¹¹Hosting Certification Framework, March 2021 v2: *jurisdiction* zero on an extraction where *certification* returns 104. See Appendix A, item 7.

¹²Commonwealth Procurement Rules 2025: *jurisdiction* zero on an extraction where *procurement* returns 336. See Appendix A, item 8.

¹³ASD, *IRAP Policy and Procedures v2.0*, §4.1.1, printed page 14. See Appendix A, item 9.

That framework carries one requirement in this territory. **IRAP-AR-0019**, printed under the heading *Coverage*, dated Apr 2025, at printed page 19:

“The IRAP assessment report covers aspects regarding data sovereignty, off-shore equipment and staff, or any information (including metadata) that is not within Australia.”¹⁴

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

This is a coverage requirement and it is mandatory. An assessor who reports on all three limbs has met it. **Nothing in this supplement suggests otherwise, and nothing here is a finding about any assessor.**

Across IRAP Policy and Procedures, *jurisdiction*, *foreign* and *compel* do not occur. Across the Common Assessment Framework, they do not occur either.¹⁵

04 Where the instruments send a reader next

Six referrals were followed one step each.

- **PSPF Direction 001-2024** points to Policy Explanatory Note 01/24 — **not publicly obtainable**.
- **PSPF Release 2025, §15.2.3** points to ASD, *Cloud assessment and authorisation* — **public**.
- **PSPF Release 2025, §15.2.3** points to ASIO T4 Protective Security Circular 149 — **not publicly obtainable**.
- **ASD, *Cloud assessment and authorisation*** points to ASIO T4 Protective Security Circular 149 — **not publicly obtainable**.
- **ASD, *Cloud assessment and authorisation*** points to NIST SP 800-145 — **public**.
- **IRAP Policy and Procedures, §4.1.1** points to the IRAP Common Assessment Framework — **public**.

Three resolve to public documents and three to two documents that are not publicly obtainable.

Two of the six referrals name a document as carrying guidance on this subject, and both name a document this practice could not obtain. PSPF Direction 001-2024 states

¹⁴ASD, *IRAP Common Assessment Framework*, IRAP-AR-0019, printed page 19. See Appendix A, item 10.

¹⁵*jurisdiction*, *foreign* and *compel* each return zero across IRAP Policy and Procedures on an extraction where IRAP returns 587, and across the Common Assessment Framework on an extraction where *assessment* returns 361. See Appendix A, items 9 and 10.

that **“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.”**¹⁶ On 11 August 2026 this practice searched for a publicly retrievable copy and did not find one; the routes tried are recorded in the published assessment. **This is a statement about what a search on that date found. It is not an assertion that the note does not exist.**

The ASD document states that **ASIO T4 Protective Security Circular 149 “(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.”**¹⁷ That document was not obtained.

The three public referrals among the six do not carry the method. The ASD document names factors without tests; the Common Assessment Framework requires coverage of location; NIST SP 800-145 is cited for terminology.

05 What this changes, and what it does not

Recommendation F stands. A methodology standard for jurisdictional exposure assessment is still the ask, and nothing established here weakens the case for it. **What changes is the model.**

The committee should not be left to infer that the pathway exists in the instruments named and needs only extending. On this question, the ISM and the PSPF name the risk, IRAP’s one requirement on the subject asks where things are, and none of them supplies, in its own text, a method for assessing it. PSPF Release 2025 §6.1.3 refers to two further documents.¹⁸ One, ASIO’s Due Diligence Integrity Tool, this practice has not obtained. The other, Home Affairs’ Foreign Ownership, Control or Influence Risk Assessment Guidance, asks whether a foreign government could compel a vendor to provide access to its data,¹⁹ but its first question routes a United States owned provider to cyber hygiene before that question is reached, as AOS-CMP-2026-001 records.²⁰ **A standard built by extending the ISM, the PSPF and IRAP would be built on the part of them that is absent.**

This supplement does not say that any framework should require more. Recommendation F already asks for the standard, and that ask is unchanged. Whether these instru-

¹⁶PSPF Direction 001-2024, printed page 1. See Appendix A, item 5.

¹⁷ASD, *Cloud assessment and authorisation*, printed page 7. See Appendix A, item 6.

¹⁸Protective Security Policy Framework, Release 2025, §6.1.3, printed pages 25 to 26. See Appendix A, item 4.

¹⁹Department of Home Affairs, *Foreign Ownership, Control or Influence Risk Assessment Guidance (without Appendices)*, Sections 1 and 2, printed page 7. See Appendix A, item 11.

²⁰AOS-CMP-2026-001 v1.4, section 4, page 7. See Appendix A, item 12.

ments ought to contain such a method is a judgement about policy this practice does not make, in either direction.

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

It does not say that any agency, provider or system is exposed. No claim is made that any data has been accessed, that any provider is subject to any foreign direction, or that any system is at risk.

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, and nothing whatever about their content.**

The eight instruments examined are those named above. The Defence Industry Security Program, Digital Transformation Agency cloud guidance, the international standards bodies' control catalogues and professional assurance standards were not reached.

The author is available to assist the committee in its consideration of these matters.

Appendix A. Sources

1. AOS-AIDC-2026-001, as lodged in this inquiry: Recommendation F.
2. AOS-ASR-2026-001, SHA-256 25f58a747e87a81158f7d3fa9e23aab80402cf1431753aa64141fbf299a8a56d, published with verification record. **Cited as a pointer to the working only; the source of no claim in this supplement.** <https://australiaos.com.au/verify/AOS-ASR-2026-001>
3. Information security manual, *Guidelines for procurement and outsourcing*, June 2026 release, 9 printed pages. Retrieved 15 August 2026; every page read at image resolution 19 August 2026. <https://www.cyber.gov.au/sites/default/files/2026-06/05.%20ISM%20-%20Guidelines%20for%20procurement%20and%20outsourcing%20%28June%202026%29.pdf>
4. Protective Security Policy Framework, Release 2025, 165 printed pages. Retrieved 5 August 2026. <https://www.protectivesecurity.gov.au/system/files/2025-07/pspf-release-2025.pdf>
5. PSPF Direction 001-2024, *Managing Foreign Ownership, Control or Influence Risks in Technology Assets*, 2 printed pages. Retrieved 11 August 2026. <https://www.protectivesecurity.gov.au/system/files/2024-07/PSPF%20Direction%20001-2024.pdf>
6. Australian Signals Directorate, *Cloud assessment and authorisation*, January 2024, 26 printed pages. Retrieved 19 August 2026. <https://www.cyber.gov.au/sites/default/files/2024-01/Cloud%20assessment%20and%20authorisation.pdf>



- ault/files/2025-03/Cloud%20assessment%20and%20authorisation%20%28January%202024%29.pdf
7. Hosting Certification Framework, March 2021 version 2. Retrieved 5 August 2026. <https://www.hostingcertification.gov.au/sites/default/files/2021-11/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf>
 8. Commonwealth Procurement Rules 2025, 36 printed pages. Retrieved 11 August 2026. <https://www.finance.gov.au/sites/default/files/2025-10/Commonwealth-Procurement-Rules-2025.pdf>
 9. Australian Signals Directorate, *IRAP Policy and Procedures*, version 2.0, 29 printed pages. Retrieved 31 July 2026. <https://www.cyber.gov.au/sites/default/files/2026-05/IRAP%20Policy%20%26%20Procedures%202026.pdf>
 10. Australian Signals Directorate, *IRAP Common Assessment Framework*, 36 printed pages. Retrieved 31 July 2026. <https://www.cyber.gov.au/sites/default/files/2026-05/IRAP%20common%20assessment%20framework.pdf>
 11. Department of Home Affairs, *Foreign Ownership, Control or Influence Risk Assessment Guidance (without Appendices)*, 21 printed pages. Retrieved 5 September 2026; Sections 1 and 2 read at image resolution 6 October 2026. <https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-without-appendices.pdf>
 12. AOS-CMP-2026-001 v1.4, SHA-256 d964c1ad31d43a788bd579430bd72483f5662ec895063eda45bc241a8dce4b5d, published with verification record. Cited for its section 4. <https://australiaos.com.au/verify/AOS-CMP-2026-001>

Every source above was retrieved by this practice and hashed on retrieval. The hashes and retrieval times are recorded in the verification record of AOS-ASR-2026-001, published with that assessment, and for item 11 in that of AOS-CMP-2026-001.

Nothing above is cited from memory. —

End of supplement.