Stated, Not Required

REFERENCE	AOS-ISM-2026-001
VERSION	1.1
DATE	19 August 2026
CLASSIFICATION	Released
DIRECTOR	Brunel Al-Bijwaie

Version 1.1, 19 August 2026. This assessment examines one chapter of one published guidance document, in two releases. It rests entirely on those releases' own text. **Control citations give the control number, revision and applicability exactly as the document prints them.** Page citations give the printed page number.

Version note

This is v1.1, published 19 August 2026. It is a correction to v1.0 of 17 August 2026. **Two figures change and one sentence is withdrawn. No finding moves, and nothing else in v1.0 is withdrawn or qualified.**

Where	What changed	Why
Section 5, first sentence	"The chapter carries **39** controls in the June 2026 release" becomes **38**	The chapter carries 38. Counted at this revision by rendering all nine pages and counting the printed control entries: 2+9+4+2+5+3+11+2+0. **No identifier appears in a heading, table, appendix or cross-reference**
Section 7, the control comparison	"March carries 38 controls, June 39. **ISM-0138 entered the chapter**" is withdrawn and replaced. **The control set is unchanged: 38 in each release, and the two sets are identical**	ISM-0138 is in neither release of this chapter. The set difference is empty in both directions
Section 7, the change log paragraph	"**All eight** controls that moved or entered this chapter are named in it" becomes **all seven**, and the eighth identifier is explained	Seven controls' revisions moved in this chapter. The change log's closing minor-grammar list names those seven **and** ISM-0138, which belongs to another chapter
Section LM	"**One figure** rests on extraction rather than on reading" becomes **five**, each named	The declared limitation was true of more than one number, and v1.0 named only the one

Where the error came from. Not from the extractor. **Repeating v1.0's own test today returns 38 across four extraction methods**, and v1.0's own arithmetic already gave 38 — seven revisions moved plus thirty-one identical. **39 came from reading the June change log's closing list as though every identifier in it concerned this chapter.**

How it was found. By rendering the chapter's pages and counting the printed entries on 19 August 2026, during the pre-publication audit of a different assessment that cites the same chapter, **before any external party raised it.**

What Section 7's proposition still holds, and why it is narrower and better evidenced. The section's proposition is about the change log: it records changes at control level and does not record changes to narrative text. **That is unaffected.** And with the control sets now established as identical, **the narrative addition is the only substantive change to this chapter between the two releases** — which is the one change the change log does not record.

The finding does not move. Section 7 states on its own face that nothing in Sections 3 to 6 depends on it. The finding is that the chapter states the risk in narrative and requires nothing about it in any control, and that holds at 38 and at 39 and in both releases.

The full account, with its reach determination, is in `CORRECTIONS-REGISTER.md`.

v1.0 remains published at its own address with its own hash, and both versions resolve.

1. Scope

This assessment examines the *Guidelines for procurement and outsourcing* in the Australian Signals Directorate's **Information security manual**, in the **June 2026** release and, for one comparison only, the **March 2026** release.

The Information security manual is guidance. It is not a legislative instrument. A full-text search of the Federal Register of Legislation for "Information security manual" returned a results page carrying **no occurrence of that title**. The manual is published by the Australian Signals Directorate on cyber.gov.au. **This bounds what the word "requires" can mean anywhere in this document: a control "requires" something in the sense that the manual states it as a control, not in the sense that a statute imposes it.** Nothing here should be read as a statement about legal obligation.

The question this assessment puts is narrow. The chapter's opening narrative names foreign lawful access to data. **Does any control in the chapter require an organisation to establish whether a supplier is subject to it?**

The domain, stated before the finding rather than after it.

- **Read in full:** the *Guidelines for procurement and outsourcing* chapter in both releases, end to end. The June 2026 release change log, six printed pages. The manual's own "Select controls" and "Assess controls" sections, printed pp 2–3.
- **Read in part:** the June 2026 full release, 261 printed pages — searched exhaustively for one control number across four extraction methods, and read at the sections named above. **It was not read end to end.**
- **Not read:** every other chapter of either release, except where searched for a single control number.
- **Available and not retrieved: seven earlier releases.** The publisher's archived-releases index publishes releases from June 2024 onward as ZIP archives. **Only March 2026 and June 2026 were retrieved. This assessment says nothing about any release before March 2026.**

The releases are quarterly, established from that index: March, June, September and December, across 2024 to 2026.

---

2. Two things a reader could conflate

This document carries **two propositions**, and they are independent.

The first is about the instrument as it stands. The June 2026 chapter states something in its narrative and requires something narrower in its controls. **This proposition does not depend on anything having changed.** If nothing had moved between March and June, every word of it would stand.

The second is about a change between two releases. One phrase entered the narrative sentence between March and June 2026, and the release change log does not record it.

They are set out separately, at Sections 3 to 6 and at Section 7, and neither rests on the other. A reader who rejects the second entirely is left with the first intact.

---

3. What the chapter states

The chapter opens under the heading "Cyber supply chain risk management". Its narrative reads, in the June 2026 release:

> "Furthermore, this also includes identifying and managing jurisdictional, governance, privacy and security risks associated with the use of suppliers, such as software developers, IT equipment manufacturers, OT equipment manufacturers, service providers and other organisations involved in distribution channels. For example, outsourced artificial intelligence applications or cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge. Additionally, use of offshore services introduces jurisdictional risks as foreign countries' laws could change with little warning. Finally, foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers."

Three propositions are stated there: that offshore services may be subject to lawful and covert data collection without their customers' knowledge; that foreign countries' laws may change with little warning; and that **foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.**

The third is the proposition this assessment is about. The manual names it. That is not in question anywhere in this document.

---

4. Why that passage is narrative, and what that means here

Every control in this chapter is printed with four fields on one line, in this form:

> "Control: ISM-1452; Revision: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A"

The passage quoted at Section 3 carries none of the four. It has no control number, no revision, no "Updated" month, no applicability marking and no Essential Eight mapping. **That is the document's own typography, not a characterisation applied to it from outside.**

The manual describes the relationship in its own words, in the section titled "Select controls", printed p 2:

> "Each cyber security guideline discusses security risks associated with the topics it covers. Paired with these discussions are controls that ASD considers to provide efficient and effective mitiga-

> tions based on their suitability to achieve the security and resilience objectives for a system. To assist with selecting and tailoring controls for a system, each control is assigned an applicability marking."

And in "Assess controls", printed p 3:

> "Generally, the scope of the security assessment will be determined by the type of system and the controls implemented for the system and its operating environment."

So the manual's own structure is: guidelines discuss risks; controls are paired with those discussions; controls carry applicability markings, are documented in the system security plan annex, are approved by the authorising officer, and are what a security assessment's scope is determined by.

The limit on that, stated rather than glossed over. The manual nowhere says that its narrative text is non-binding, or that narrative carries no weight. It does not use those words or any equivalent. The distinction drawn above is **structural** — it is about what the manual does with controls — and it is not a statement by ASD that discussion may be disregarded. **This assessment asserts the structure and does not assert the sharper claim.** A reader who thinks the narrative carries obligations of its own will find nothing here that contradicts them; what follows is about the controls.

---

5. What the controls require

The chapter carries 38 controls in the June 2026 release. Seven follow the narrative passage before the next heading, and all seven are quoted here, with their own fields:

> "Control: ISM-1631; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Suppliers of operating systems, applications, IT equipment, OT equipment and services associated with systems are identified."

> "Control: ISM-1452; Revision: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A — A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services to assess the impact to a system's security risk profile."

> "Control: ISM-1567; Revision: 2; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Suppliers identified as high risk by a cyber supply chain risk assessment are not used."

> "Control: ISM-1568; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to the security of their products and services."

> "Control: ISM-1882; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Operating systems, applications, IT equipment, OT equipment and services are pro-

> cured from suppliers that have demonstrated a commitment to transparency for their products and services."
>
> "Control: ISM-1632; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems."
>
> "Control: ISM-1569; Revision: 3; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A — A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party."

They require identification, assessment, sourcing and a shared responsibility model. None of them requires an organisation to establish whether a supplier is subject to a foreign government's lawful access.

That absence was established by reading, not by searching. The chapter runs from printed p 26 to p 33 in the June release. **From the section headed "Managed services and cloud services" to the end of the chapter, no passage contains the words foreign, jurisdiction, offshore, overseas, lawful, covert, sovereign, or "outside Australia".** Every occurrence of that vocabulary in the chapter is in the narrative quoted at Section 3.

---

6. The contrast

This is the finding, and it is a contrast rather than an absence.

For managed services and cloud services, the same chapter specifies who performs the assessment, against what, and how often.

> "Control: ISM-1793; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A — Managed service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services undergo an Infosec Registered Assessor Program (IRAP) assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months."
>
> "Control: ISM-1971; Revision: 0; Updated: Dec-24; Applicable: TS; Essential 8: N/A — Managed service providers and their TOP SECRET managed services, including sensitive compartmented information managed services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months."

ISM-1570 and ISM-1972 carry the same two provisions for outsourced cloud services, at the same revisions and dates.

For the supply chain risk assessment, the chapter specifies none of the three.

- **No performer.** ISM-1452 reads "A supply chain risk assessment **is performed**". The verb is passive and **no actor is named**.
- **No standard or criteria.** ISM-1567 turns on suppliers "identified as **high risk**", and **the chapter nowhere says what makes a supplier high risk.**
- **No cadence.** Nothing states when, or how often.
- **No output.** No report, record or register is required of it. **The same chapter does require registers elsewhere** — a managed service register at ISM-1736 and an outsourced cloud service register at ISM-1637, each "developed, implemented, maintained and regularly verified".
- **No review, test or assurance.** The words reviewed, verified, assured and audited appear in the chapter only for those two registers and for contractual rights to verify compliance. **They are never applied to the supply chain risk assessment.**

Those five are established of ISM-1452, the control that requires the assessment. ISM-1567 is a different kind of control and not all five apply to it. ISM-1567 prohibits an outcome — "Suppliers identified as high risk... are not used" — rather than requiring an activity, so cadence and output are not properties it could have. **What is established of ISM-1567 is narrower and is stated as such: the term "high risk" on which it turns is nowhere defined in the chapter, and the identification it relies on is the same assessment, which has no named performer and is subject to no review, test or assurance. Nothing beyond that is asserted of it.**

The manual's general account of assessors does not reach it either. That account, quoted at Section 4 and set out at printed p 3, is framed throughout on systems: "the assessor, **system owner** and authorising officer"; "the type of **system** and the controls implemented"; "For TOP SECRET **systems**... For non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET **systems**, security assessments can be undertaken by an organisation's own assessors or Infosec Registered Assessors Program (IRAP) assessors."

The assessment ISM-1452 requires is of suppliers, not of a system's controls. The phrase "supply chain risk assessment" occurs exactly twice in the 261 printed pages of the June 2026 release — at ISM-1452 and ISM-1567, both in this chapter — **and is nowhere defined.**

---

7. What changed between March and June 2026

This section is the second proposition. Nothing in Sections 3 to 6 depends on it.

The narrative sentence gained three words.

March 2026:

> "For example, outsourced cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge."

June 2026:

> "For example, outsourced artificial intelligence applications or cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge."

The inserted words are "artificial intelligence applications or". Nothing else in that sentence moved.

The chapter's controls, March against June. The control set is unchanged. Each release carries 38 controls and the two sets are identical: no control entered the chapter and none was removed. Seven controls' revisions moved, all to Jun-26: ISM-0072 (9 to 10), ISM-1452 (6 to 7), ISM-1569 (2 to 3), ISM-1574 (3 to 4), ISM-1637 (2 to 3), ISM-1736 (1 to 2), ISM-1738 (1 to 2). **Thirty-one were identical in all four printed fields, and thirty-one plus seven is thirty-eight. No applicability changed and no Essential Eight mapping changed. The only substantive change to this chapter between the two releases is in its narrative text**, which is what the rest of this section examines.

Elsewhere in the narrative, "In particular, an organisation should consider the [risks] that may arise" became "This includes considering", "This" became "Furthermore, this also", and "foreign owned" became "foreign-owned".

What the change log records, and what it does not

ASD publishes a change log with each release. The June 2026 change log runs to six printed pages, is organised by chapter, and cites affected control numbers in brackets after each described change.

Its chapter headings are: cyber security principles, cyber security documentation, personnel security, enterprise mobility, media, system hardening, software development, and cryptography. "Guidelines for procurement and outsourcing" is not among them.

All seven controls whose revisions moved in this chapter are named in it — ISM-0072, ISM-1452, ISM-1569, ISM-1574, ISM-1637, ISM-1736 and ISM-1738 — each once, in a closing list introduced by the words "Minor grammar corrections were made to principles and controls that did not affect their intent." **That list names an eighth identifier, ISM-0138, which is in neither release of this chapter**; it appears in the March release in the *Guidelines for cyber security incidents*.

The addition of "artificial intelligence applications" to the narrative is not recorded anywhere in it.

What that establishes is about the change log: it records changes at control level and does not record changes to narrative text. **A reader relying on it to learn what moved between the two releases would not learn that this phrase had been added. Nothing here is an allegation that anything was concealed**, and this assessment does not suggest one. The change log describes what it describes; this records what a reader would and would not find in it.

---

8. The finding

In the Guidelines for procurement and outsourcing, June 2026 release, the Information security manual states that foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers, and no control in that chapter requires an organisation to establish whether any particular supplier is.

The chapter requires a supply chain risk assessment (ISM-1452) and specifies no performer, no criteria, no cadence, no output and no assurance for it — while specifying a performer, a standard and a cadence, in the same chapter, for the IRAP and ASD assessments of managed services and cloud services.

It further requires that suppliers identified as high risk not be used (ISM-1567) without defining high risk anywhere in the chapter. That is a narrower statement than the one above and is made separately, because ISM-1567 prohibits an outcome rather than requiring an activity: cadence and output are not properties it could have.

LM · Limitations of this assessment

It is bounded to one chapter of one document, in two releases. The June 2026 release runs to 261 printed pages. **Only this chapter was read end to end**, together with the manual's own "Select controls" and "Assess controls" sections. **A control elsewhere in the manual requiring what this chapter does not would defeat the finding, and no such search of the whole manual was performed.**

It says nothing about releases before March 2026. Seven are published and were not retrieved.

It does not say the ISM should require anything. Whether the manual ought to contain such a control is a judgement about policy, and this assessment does not make it, in either direction.

It does not say any organisation failed to consider foreign lawful access. An organisation performing a supply chain risk assessment may consider anything it wishes, and many will. **The finding is about what the instrument requires, not about what anyone did.**

It makes no finding about the Australian Signals Directorate, about the Infosec Registered Assessors Program, about any assessor, or about any supplier. Sections 4 and 6 quote the manual on who may perform assessments; those are quotations of the instrument and are not findings about the parties named.

It does not say the narrative passage is without effect. As Section 4 records, the manual nowhere says that.

"Requires" throughout means "states as a control". The manual is guidance and is not a legislative instrument.

Five figures rest on extraction rather than on reading. The March control count, the thirty-one identical in all four printed fields, the seven revision moves, the applicability and Essential Eight zeros, and the change

log's page count were each produced by matching the printed line across extracted text rather than by reading the page. **All five recompute to the values stated here, on 19 August 2026. Recomputation is not reading**, and a defect an extraction reproduces consistently would survive it. The June control count was extraction-derived at v1.0 and **is read at this revision**, from nine rendered page images; the seven quoted controls and the four registers were read directly at v1.0.

Related published assessments

`AOS-CMP-2026-001` examined two Commonwealth instruments administered by the Department of Home Affairs and found that neither tests whether a certified provider can be lawfully compelled by a foreign government to disclose the data it holds. `AOS-ACD-2026-001` examined a vendor question set in Australian Signals Directorate guidance and found that a question group headed for data sovereignty asks where data is and does not ask whose law reaches the vendor holding it.

They are cited for those two findings and no more. The instrument examined here is a third, of a different kind, and this assessment neither supersedes nor extends them. It sits beside them, and it differs from both in one respect worth stating plainly: this instrument does name foreign lawful access. The finding here is not that the question is unnamed. It is that naming it in narrative and requiring it in a control are different things, and this chapter does the first.

End of document.