



Stated, Not Required

REFERENCE	AOS-ISM-2026-001
VERSION	1.2
DATE	5 September 2026
CLASSIFICATION	Released
DIRECTOR	Brunei Al-Bijwaie

Version 1.2, 5 September 2026. This assessment examines one chapter of one published guidance document, in three 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 v1.2, published 5 September 2026. It follows the September 2026 release of the manual, first published 3 September 2026, and it follows AOS-ICL-2026-001, published 4 September 2026. **It is a revision after a new release of the instrument, and this is what such a revision is:**

- **Three statements in v1.1 were wrong when made, and two of them were also in v1.0.** All three are withdrawn here and replaced. None moves the finding.
- **One statement was true without ground at its width and is narrowed.** Section 4’s sentence on what the manual nowhere says now states the sections read and the terms searched for.
- **One limitation narrows and is not removed.** v1.1 said no search of the whole manual had been performed. One has now been performed over the description of every control in the manual, in June and in September, and its limit is stated with it at Section LM.
- **The finding is re-established on each limb against the September 2026 release,** at Sections 3, 5, 6 and 8.
- **The June figures stand as June figures.** The chapter’s 38 controls, its seven revision moves, its 31 controls identical across March and June, and the vocabulary result over the June chapter are unchanged and are not restated as September figures.
- **The release-to-release finding is AOS-ICL-2026-001’s** and is cited at the end of this document, not restated.

Where	What changed	Why
Version note, v1.1	<i>“the narrative addition is the only substantive change to this chapter between the two releases”</i> is withdrawn	A second narrative passage changed between March and June 2026, in the passage on data ownership. Section 7 quotes both releases. This statement was in v1.1 only

Where	What changed	Why
Section 6, the fifth bullet	<i>“The words reviewed, verified, assured and audited appear in the chapter only for those two registers and for contractual rights to verify compliance”</i> is replaced by the counts	“Reviewed” appears once, at ISM-0072, for contractual security requirements, which is neither a register nor a right to verify compliance. This statement was in VI.0 and VI.I. The bullet’s closing clause, that none of these words is applied to the supply chain risk assessment, was true and stands
Section 6, the assessment controls	<i>“ISM-1570 and ISM-1972 carry the same two provisions for outsourced cloud services, at the same revisions and dates”</i> becomes the four revisions and dates as printed	ISM-1793 is at revision 1 and ISM-1570 at revision 2; the dates are the same and one revision is not. This statement was in VI.0 and VI.I
Section 4, the limit	<i>“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”</i> is narrowed to the sections read and the terms searched for	The manual was not read end to end, so “nowhere” and “any equivalent” were wider than the reading. Not shown false; narrowed
Section 7, the June log	The sentence on the narrative addition gains its width and names the log’s one “artificial intelligence applications” heading	The heading sits under the system hardening entries
Section 1	Three releases; the domain restated	The September 2026 release was read
Section 3	The September passage beside the June one	The example sentence changed; the sentence this assessment is about did not
Section 4	The September wording of the manual’s assessor passage, noted	The term “security assessment” became “security control assessment”; the quotations are June’s

Where	What changed	Why
Section 5	September's 40 controls, the two that entered, the nearest control named, the vocabulary test re-run	The finding's second limb, re-established
Section 6	The five absences re-established in September; the two registers' contents; ISM-1971 and ISM-1972 relabelled	The finding's third and fourth limbs, re-established
Section 7	The second March-to-June change; a new subsection, June to September	The correction, and the current release
Section 8	The finding holds on each limb in September	Stated after the June finding, which stands
Section LM	The whole-manual sentence replaced by a bounded search; the earlier-releases sentence updated; the extraction list extended	The limitation narrows
Related published assessments	AOS-ICL-2026-001 added	Cited for its finding and no more

How the three withdrawn statements were found. The first by reading the pinned March and June chapters against v1.1's own text while scoping this revision, on 5 September 2026. The second the same day, by reading the fifth bullet of Section 6 beside the counts it rests on: the counts were right and the sentence claimed more than they support. The third the same day, by a sweep of this document for every sentence carrying a universal, which put the "same revisions" sentence beside the four control lines. **None was raised by any external party.** The full account of each, with its reach, is in `CORRECTIONS-REGISTER.md`.

Typography of quotations, stated once. Quotations reproduce the manual's typographic apostrophe. Where a control is printed as a bulleted list, its items are run together with semicolons. Where words are omitted inside a quotation, an ellipsis marks the omission; four passages are quoted so: the controls ISM-1567 and ISM-2125 and the manual's assessor passage at Section 6, and the two register items quoted at Sections 5 and 6, where the ellipsis stands for the service each names. No quotation stops before the end of its sentence or its list.

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

Version note — vi.1, 19 August 2026

Carried verbatim from vi.1. One sentence in it, on the only substantive change between the two releases, is withdrawn at vi.2, as the version note above records; the two other withdrawn statements are in the body, not in this note.

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

Where the error came from. Not from the extractor. **Repeating vi.0’s own test today returns 38 across**

four extraction methods, and v1.o'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.o 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, with the **March 2026** release for one comparison and the **September 2026** release, first published 3 September 2026, read for whether the finding holds in the current 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 all three releases, end to end, the September chapter on its ten rendered pages as well as in its text. The June 2026 release change log, six printed pages. The September 2026 change log's section for this chapter and its “Miscellaneous” section; the log's ten pages were searched entire for three phrases and not otherwise read. The manual's own “Select controls” and “Assess controls” sections in the June release, printed pp 2–3, and the “Assess security controls” section in the September release.
- **Read in part:** the June 2026 full release, 261 printed pages, and the September 2026 full release, 271 printed pages — each searched exhaustively for one phrase, and the June release for one control number across four extraction methods. The description of every control in each release was read through the publisher's own control list, 1,101 controls in June and 1,143 in September, for seven terms; the eleven controls that match were read in full. **Neither release was read end to end.**
- **Not read:** every other chapter of any release, except where searched for a single control number or phrase.
- **Seven releases before March 2026 are published.** This assessment says nothing about them. AOS-ICL-2026-001 reads them.

The releases are quarterly, established from the publisher's archived-releases 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.”

In the September 2026 release the same passage reads, quoted from the same sentence of the same paragraph to its end:

“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, managed services or outsourced 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.”

The example changed, from “outsourced artificial intelligence applications or cloud services” to “managed services or outsourced cloud services”. **The other three sentences are unchanged, word for word.**

Three propositions are stated there, in both releases: 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, in June and in September. 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 June 2026 release, 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 mitigations 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.”

In the September 2026 release that section is headed “Assess security controls” and the sentence reads:

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

The term changed; the structure did not. The quotations in this section and at Section 6 are the June wording.

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. In the sections read, the manual does not say that its narrative text is non-binding or that narrative carries no weight, and a search of the whole June and September 2026 releases for the terms “non-binding”, “not binding”, “no weight” and “not

mandatory” returns none of them in either; “binding” alone occurs zero times in June and once in September, in a sentence on cryptographically binding authentication artefacts to devices. The search reads the text it searches: “do not represent the full extent”, from the manual’s own sentence on its guidelines, returns once in each release. Whether the manual says so in other words in a chapter not read was not established. 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 procured 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.

In the September 2026 release the chapter carries 40 controls, counted at this revision by rendering all ten pages and counting the printed control entries: 2+9+4+2+4+3+12+4+0+0. **The seven quoted above are printed identically in September, in all four fields and in their text.** Two controls entered, both under the heading “Access to systems by service providers”, and none left:

“Control: ISM-2124; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A — Access by a service provider to an organisation’s systems is restricted to remote management tools, source network addresses and time windows explicitly approved by the organisation.”

“Control: ISM-2125; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A — All access to an organisation’s systems by a service provider is independently logged by the organisation in a manner that the service provider cannot modify or delete, and analysed in a timely manner to detect any anomalous, unexpected or unauthorised activity.”

Five controls carry a new revision in September, all dated Sep-26: ISM-1576 (4 to 5), whose text gains one clause, quoted at Section 7; and ISM-1638 (3 to 4), ISM-1737 (1 to 2), ISM-1971 (0 to 1) and ISM-1972 (0 to 1), whose text changes are the term “security assessment” becoming “security control assessment” and, in the two register controls, “point of contact for users of the ... service” becoming “organisational point of contact for the ... service”. **The other 33 are identical in all four printed fields, and $33 + 5 + 2 = 40$.**

Neither of the two that entered requires an organisation to establish whether a supplier is subject to a foreign government’s lawful access. ISM-2124 restricts the tools, source addresses and time windows through which a service provider may reach a system; ISM-2125 has that access logged and analysed. Neither names a jurisdiction, a law or a foreign government.

The nearest control in either release is named here so that a reader does not find it first. It is printed identically in June and September:

“Control: ISM-1572; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A — The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.”

It has a location documented. It asks nothing about whose law reaches the provider that holds the data there.

The 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 June chapter, no passage contains the words foreign, jurisdiction, offshore, overseas, lawful,**

covert, sovereign, or “outside Australia”. Every occurrence of that vocabulary in the June chapter is in the narrative quoted at Section 3.

The same test over the same range of the September chapter returns one occurrence, of “outside Australia”, and it is in narrative, under the heading “Access to systems by service providers”:

“However, without appropriate measures in place, such access could leave systems vulnerable, especially when access originates outside Australia or involves privileged administrative activities.”

The June sentence at the same place reads:

“However, without proper controls in place, this could leave systems vulnerable – especially when access occurs from outside of Australian borders.”

The June test did not match that sentence and v1.1 did not name it. It is named now. In both releases the sentence is narrative and not a control, and in both it concerns where a service provider’s access comes from, not whose law reaches the provider. **The other seven terms return zero over that range in September as in June, and the test reads the text it searches: over the whole September chapter the same terms return foreign 3, jurisdiction 2, offshore 2, lawful 2 and covert 1, every one of them in the passage 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. In the June 2026 release:

“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. In the June 2026 release all four are dated Dec-24: ISM-1793 is at revision 1 and ISM-1570 at revision 2; ISM-1971 and ISM-1972 are both at revision 0. **In the September 2026 release ISM-1793 and ISM-1570 are unchanged; ISM-1971 and ISM-1972 are at revision 1, Sep-26, and read “security control assessment” in the two places where**

June reads “security assessment”, with performer, standard and cadence unchanged.

For the supply chain risk assessment, the chapter specifies none of the three, and this is so in June and in September, where ISM-1452 and ISM-1567 are printed identically in all four fields and in their text.

- **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**. The words “high risk” occur once in the chapter, at ISM-1567 itself, in June and in September.
- **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.** In the June 2026 chapter, “verified” appears twice, at the two registers, which are “regularly verified” (ISM-1736, ISM-1637); “reviewed” appears once, at ISM-0072, where contractual security requirements are “regularly reviewed to ensure they remain fit for purpose”; “verify” appears twice, at ISM-1571 and ISM-1738, for the contractual right to verify compliance; “assured” and “audited” do not appear. The counts are the same in the September 2026 chapter. ISM-2125, added in September, has service-provider access “independently logged ... and analysed”; that attaches to access. **None of these is applied to the supply chain risk assessment.**

What the two registers must hold is specified beside them, and neither item list reaches the provider as a legal entity. In the September 2026 release, with its list run together:

“Control: ISM-1638; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A — An outsourced cloud service register contains the following for each outsourced cloud service: cloud service provider’s name; cloud service’s name; purpose for using the cloud service; sensitivity or classification of data involved; due date for the next security control assessment of the cloud service; contractual arrangements for the cloud service; organisational point of contact for the cloud service; 24/7 contact details for the cloud service provider.”

ISM-1737 (revision 2, Sep-26) lists the same eight items for a managed service and its provider. In June both controls list eight items too, at their earlier revisions, reading “security assessment” and “point of contact for users of the ... service”. **Eight items each, in both releases; none concerns the provider’s jurisdiction, incorporation or legal entity, and the only item about the provider as an entity is its name.**

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 in its June wording 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.” **In September the same account reads “security control assessment” and “security control assessments” in those places, and is framed on systems in the same words.**

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. It occurs exactly twice in the 271 printed pages of the September 2026 release, at the same two controls; the same search over the September release, its text layer read with line breaks collapsed, returns “security control assessment” 47 times, so it reads the text it searches.

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.

A second narrative passage changed in the same pair, and VI.0 and VI.1 did not record it. Under the heading “Contractual security requirements with service providers”:

March 2026:

“In addition, although data ownership resides with service providers’ customers, this can become less clear in some circumstances, such as when legal action is taken and a service provider is asked to provide access to, or data from, their assets.”

June 2026:

“In addition, although data ownership resides with service providers’ customers, this can become less clear in some circumstances, such as when a service provider is legally required to provide access to, or data from, their assets.”

The occasion widened, from legal action in which a provider is asked, to any legal requirement on the provider. VI.1’s version note described the three inserted words as the only substantive change to this chapter between the two releases. **That sentence is withdrawn at this revision.** The June sentence is printed unchanged in September.

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 seven were read in both releases.** Each is a wording edit and nothing else: “in order to” became “to” (ISM-1452, ISM-1569); “allows for” became “enables” (ISM-1574); “verified on a regular basis” became “regularly verified” (ISM-1637, ISM-1736); and “reviewed on a regular and ongoing basis” and “exercised on a regular and ongoing basis” became “regularly reviewed” and “regularly exercised” (ISM-0072, ISM-1738). None changes who acts, what is acted on, or how often. **The only substantive change to this chapter between the two releases is in its narrative text,** which is what 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: “artificial intelligence applications or cloud services” occurs zero times in the log’s six pages, and “artificial intelligence applications” occurs once, as a heading under the system hardening entries, above two new controls on AI applications in that chapter, ISM-2112 and ISM-2113. **Nor is the change to the data-ownership sentence:** “legally required” occurs zero times in the six pages, while the log’s own introducing sentence, “Minor grammar corrections were made to principles and controls that did not affect their intent”, occurs once, so the search reads the log.

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 either passage had changed. 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.

What changed between June and September 2026

The September 2026 release is the current release, first published 3 September 2026. Two things are recorded here and no more; the question of what the manual’s record of change records, release by release, is AOS-ICL-2026-001’s.

One. The example in the narrative sentence changed again, from “outsourced artificial intelligence applications or cloud services” to “managed services or outsourced cloud services”, as quoted at Section 3. The September 2026 change log runs to ten printed pages and, unlike June’s, has a section headed “Guidelines for procurement and outsourcing”. **That section carries three entries, each citing one control identifier: ISM-2124, ISM-1576 and ISM-2125,** the two controls that entered and the one whose text changed. The four controls whose revisions moved for a change of term — ISM-1638, ISM-1737, ISM-1971 and ISM-1972 — are named in the log’s “Miscellaneous” section. **The narrative change is not recorded:** “managed services or outsourced cloud services” and “artificial intelligence applications or cloud services” each occur zero times in the log’s ten pages, while “treated as a cyber security incident”, the words of the log’s own ISM-1576 entry, occurs once, so the search reads the log.

Two. ISM-1576’s text gained one clause. June: “If an organisation’s systems are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.” September: “If an organisation’s systems are accessed or administered by a service provider in an unauthorised manner, it is treated as a cyber security incident and the organisation is immediately notified.” The passage under “Access to systems by service providers” was rewritten and grew, and the sentence quoted at Section 5 is part of it.

What three change logs record across ten releases of this chapter is AOS-ICL-2026-001’s finding, cited at the end of this document and not restated.

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.

In the September 2026 release, first published 3 September 2026, the finding holds on each limb. The sentence naming foreign lawful access is printed unchanged. ISM-1452 and ISM-1567 are printed unchanged in identifier, revision, date and text, and the five absences are re-established at Section 6. Of the two controls added to the chapter, neither requires an organisation to establish whether a supplier is subject to a foreign government's lawful access; they restrict and log a service provider's access.

LM • Limitations of this assessment

It is bounded to one chapter of one document, in three releases. The June 2026 release runs to 261 printed pages and the September 2026 release to 271. **Only this chapter was read end to end**, together with the manual's own "Select controls" and "Assess controls" sections in June and "Assess security controls" in September. **A control elsewhere in the manual requiring what this chapter does not would defeat the finding.** At this revision the description of every control in the manual was searched, through the publisher's own control list, for the terms foreign, lawful, jurisdiction, sovereign, incorporat, legal entity and countr, without regard to case: **1,101 controls in the June 2026 list, eleven matching; 1,143 in the September 2026 list, the same eleven matching and no others** — ISM-0409, ISM-0411, ISM-0420, ISM-0446, ISM-0447, ISM-1088, ISM-1535, ISM-1554, ISM-1556, ISM-1640 and ISM-1773. Each was read in full. They restrict foreign nationals' access and privileged access to systems holding AUSTEO, REL or AGAO data; identify foreign-national personnel on such systems; have personnel report credentials provided to, or devices decrypted for, foreign government officials; prevent export of AUSTEO, AGAO and REL data to unsuitable foreign systems; concern travel to high or extreme risk countries; label cables for foreign systems; and require gateway administrators for Australian Government Access Only networks to be Australian nationals or seconded

foreign nationals. **None names a supplier, a service provider or a jurisdiction of incorporation.** Nine are identical in both lists, and ISM-0409 and ISM-0411 gain the word “security” before “controls” in September. The search reads the list it searches: “foreign” alone returns nine controls in each. **The search is over control descriptions, not narrative, and not over either release end to end; a control requiring it in words the seven terms do not match would not be found by it. The limitation narrows, and it is not removed.**

It says nothing about releases before March 2026. Seven are published. AOS-ICL-2026-001 reads them, and this assessment does not.

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 does not say that in the sections read or in the terms searched for.

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

Five June 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 and again on 5 September 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 v1.1**, from nine rendered page images; the seven quoted controls and the four registers were read directly at v1.0.

The September figures rest on extraction in the same way, except one. The five revision moves and the 33 identical controls, the two occurrences of “supply chain risk assessment” in 271 pages, the word counts at Sections 5 and 6, and the change logs’ zero counts were each produced by matching extracted text, and each recomputes on 5 September 2026. **The September control count of 40 was read from ten rendered page images,** and the two controls that entered, the five that moved and the two register lists were read from those pages. The search over control descriptions reads cells of the publisher’s spreadsheet, not extracted text.

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.

AOS-ICL-2026-001 examined ten quarterly releases of this chapter, June 2024 to September 2026, and the three release change logs held, and found that for the three release pairs whose change log is held every control change in the chapter is cited in that log, and that no narrative change in the chapter is recorded in any of the three. **It is cited for that finding and no more.** This assessment reads one of those narrative changes for what it says; that assessment counts them.

End of document.