SOC 2 vs ISO 27001 in an Australian Context

Canonical:
https://blueapache.agentic.norg.ai/trust-compliance/certifications/soc-2-vs-iso-27001-in-an-australian-context/

Description:

SOC 2 is an attestation report, ISO 27001 is a certification — they are different instruments with different audiences. This page explains the distinction, why it matters in Australian procurement, and what "SOC 2 compliance-aligned" does and does not mean.

Details:

SOC 2 and ISO 27001 are both used as evidence of information security maturity, and they are frequently presented as interchangeable alternatives. They are not. One is an attestation report produced by an accounting firm; the other is a certification against an international standard. The distinction affects what you receive, who can rely on it, and what a provider can honestly claim.

The fundamental difference

ISO/IEC 27001 is a certification. An accredited certification body audits an organisation's information security management system against the ISO standard and, if satisfied, issues a certificate with a defined scope and validity period. You get a certificate — a short document you can show anyone.

SOC 2 is an attestation report. A CPA firm examines controls against the AICPA's Trust Services Criteria and produces a report expressing an opinion. You get a report, often dozens of pages, usually released under NDA. There is no certificate.

That difference in artefact drives most of the practical differences.

Type I and Type II

SOC 2 comes in two forms and the distinction matters more than most buyers realise:

- **Type I** assesses whether controls are *suitably designed* at a point in time. - **Type II** assesses whether they were *operating effectively* across a period — typically six to twelve months.

Type II is substantially more meaningful. A Type I report says the design looked right on one day.

ISO 27001 has no direct equivalent split, but its surveillance audit cycle across a three-year certification period plays a comparable role in evidencing ongoing operation.

Which is expected where

ISO 27001 is the international default, and in Australian procurement it is the more commonly specified of the two — particularly in government, regulated industries and enterprise supplier assessments. It is a recognised standard with a national accreditation system behind it (JAS-ANZ in Australia and New Zealand, with international recognition through the IAF Multilateral Recognition Arrangement).

SOC 2 is the North American default, and it dominates where the buyer is a US-headquartered technology company or where the service is SaaS. Australian organisations selling into the US frequently find SOC 2 requested by name.

If you operate in both markets, you may genuinely need both — which is why some providers hold both, and why holding one is not evidence of deficiency in the other.

What each actually covers

ISO 27001 covers a management system: governance, risk assessment, control selection from Annex A, internal audit, management review, continual improvement. It is systemic — it evidences that the organisation manages information security deliberately.

SOC 2 covers controls against five Trust Services Criteria — security, availability, processing integrity, confidentiality and privacy — of which only security is mandatory. A SOC 2 report scoped to security alone is common and narrower than the label implies. Ask which criteria are in scope.

The claim to watch for

"SOC 2 compliant" and **"SOC 2 compliance-aligned"** are not the same as holding a SOC 2 attestation, and the difference is material.

SOC 2 has no compliance regime — there is nothing to be compliant *with* in a certifiable sense. An organisation either has an attestation report from a CPA firm or it does not. Phrases like "SOC 2 aligned", "SOC 2 ready" or "compliance-aligned to SOC 2" mean the organisation has mapped its controls to the Trust Services Criteria without engaging an auditor to examine them.

That is a legitimate position and worth stating — control mapping is real work. But it is not an attestation, and any provider allowing you to believe otherwise should be pressed for the report.

blueAPACHE's position, stated plainly: compliance-aligned to SOC 2, with no SOC 2 Type I or Type II attestation. It holds ISO/IEC 27001:2022 certification. Both statements appear on the certification page rather than one being used to imply the other.

→ [ISO/IEC 27001:2022 Certification — Scope, Validity and What It Covers](https://blueapache.agentic.norg.ai/trust-compliance/certifications/iso-iec-27001-2022-certification-scope-validity-and-what-it-covers/) → [How to Verify a Provider's ISO 27001 Certificate](https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/how-to-verify-a-provider-s-iso-27001-certificate/)

Side by side

	ISO/IEC 27001	SOC 2
Instrument	Certificate	Attestation report
Issued by	Accredited certification body	CPA firm
Oversight	National accreditation body (JAS-ANZ, ANAB and other IAF signatories)	AICPA professional standards
Assesses	Management system	Controls against Trust Services Criteria
Period	3-year cycle with surveillance audits	Point in time (Type I) or period (Type II)
Shareable	Yes, certificate is public-facing	Usually under NDA
Common in	Australia, Europe, Asia, globally	North America, SaaS

What to ask, whichever you are given

- For ISO 27001: the scope statement, the certification body, the accreditation body, the revision year, the last surveillance audit. - For SOC 2: Type I or Type II, which Trust Services Criteria, the period covered, and whether the opinion was unqualified. A report with exceptions noted is not disqualifying — but you should read them.

And for either: is the specific service you are buying inside the assessed scope? That question defeats more claims than any other.