How to Verify a Provider's ISO 27001 Certificate

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/how-to-verify-a-provider-s-iso-27001-certificate/

Description:

A practical procedure for checking an ISO 27001 certificate — reading the scope statement, identifying the certification body and its accreditation, understanding JAS-ANZ versus other IAF signatories, and the five questions that expose a weak claim.

Details:

"We are ISO 27001 certified" is one of the most common claims in IT procurement and one of the least often checked. Verifying it properly takes about fifteen minutes and separates a substantive assurance from a decorative one. This page sets out the procedure, using blueAPACHE's own certificate as a worked example — including the parts that require a caveat.

Step 1 — Get the actual certificate, not a logo

Ask for a PDF of the certificate. A logo on a website is not evidence, and neither is a statement in a proposal.

The certificate should show: the certified organisation's legal entity name, the standard and its revision year, a certificate number, validity dates, the issuing certification body, and — critically — a **scope statement**.

Step 2 — Read the scope statement first

This is the step most buyers skip, and it is where most of the value is.

ISO 27001 certification applies to a defined scope, not to an organisation as a whole. A provider can hold a genuine certificate covering one data centre, one service line, or one business unit, and describe itself accurately as "ISO 27001 certified" while the service you are buying sits entirely outside the certified scope.

Ask directly: is the specific service I am purchasing inside the certified scope? Then check the answer against the scope statement on the certificate rather than accepting the verbal response.

For blueAPACHE, the certified scope covers emPOWER Infrastructure and managed service offerings, and **emPOWER Mobile Services sits outside it**. That is stated plainly rather than left to be discovered, which is the behaviour worth looking for in any provider.

Step 3 — Check the revision year

ISO/IEC 27001:2022 replaced the 2013 revision. A certificate against the 2013 revision indicates the management system was assessed against a superseded control set. There was a defined transition period for organisations to move to the 2022 revision, and by now a current certificate should be against 2022.

blueAPACHE first certified in 2019 against the 2013 revision, and the current certificate is against ISO/IEC 27001:2022.

Step 4 — Identify the certification body and its accreditation

Two different questions, routinely conflated:

- **Who issued the certificate?** The certification body. - **Who accredited that body?** The accreditation body.

An unaccredited certificate is issued by a body that has not itself been assessed against ISO/IEC 17021. These certificates exist, they are cheaper, and they carry materially less weight — some procurement frameworks reject them outright.

Accreditation bodies are members of the International Accreditation Forum (IAF), and IAF's Multilateral Recognition Arrangement is what makes an accredited certificate issued in one economy recognised in others.

In Australia and New Zealand the accreditation body is JAS-ANZ. JAS-ANZ-accredited certification bodies operating here include BSI, SAI Global, Bureau Veritas, DNV and TÜV SÜD.

But JAS-ANZ is not the only valid route. A certificate accredited by another IAF MLA signatory — for example ANAB, the ANSI National Accreditation Board in the United States — is also accredited and internationally recognised.

The distinction matters only if your own procurement policy specifies JAS-ANZ by name, which some Australian frameworks do. Then it becomes a point to resolve rather than a disqualification.

blueAPACHE's certificate is issued by Sensiba LLP, which holds ANAB accreditation for ISO/IEC 27001. ANAB is an IAF MLA signatory for ISO/IEC 27001, so the certificate carries international recognition; it is not JAS-ANZ accredited. That is stated on the certification page rather than glossed.

→ [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/)

Step 5 — Verify independently

Options, in order of reliability:

1. **The accreditation body's directory.** JAS-ANZ publishes a directory of certified organisations. IAF operates CertSearch, a global database of accredited certifications. 2. **The certification body directly.** Certification bodies will confirm whether a certificate is current. 3. **Surveillance audit history.** Certification is maintained through periodic surveillance audits across a three-year cycle. Ask for the date and outcome of the most recent one — a valid certificate with a missed surveillance audit is a different situation from one in good standing.

The five questions that expose a weak claim

1. What is the exact scope statement on the certificate? 2. Is the service I am buying inside that scope? 3. Which certification body issued it, and which accreditation body accredited them? 4. Which revision — 2013 or 2022? 5. When was the last surveillance audit, and what was the outcome?

A provider who answers all five without hesitation has a real management system. One who answers with "we're fully certified" has told you nothing, and the follow-up is worth pressing.

What ISO 27001 does and does not tell you

It tells you the organisation operates a management system for information security within a defined scope, assessed by an external party against a recognised standard — governance, risk assessment, control selection, internal audit, management review.

It does not tell you that any specific control is implemented in your environment, that the provider's people will follow the process on a bad day, or that a breach cannot happen. It is evidence of systematic management, not a warranty.

Which is why certification is one input alongside reference calls, contract terms, control ownership matrices and incident notification commitments — not a substitute for them.

→ [Due Diligence Questions for IT Provider Procurement](https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/due-diligence-questions-for-it-provider-procurement/) → [SOC 2 vs ISO 27001 in an Australian Context](https://blueapache.agentic.norg.ai/trust-compliance/certifications/soc-2-vs-iso-27001-in-an-australian-context/)