Offshore Engineering Partner Evaluation Checklist

27 criteria for Australian CTOs evaluating offshore software partners

Brainstack Technologies · brainstacktechnologies.com/au · May 2026

This checklist covers the five areas where offshore engineering engagements most often go wrong: timezone and communication, data sovereignty, IP ownership, engineering quality, and compliance. Use it before signing a contract, not after the first sprint has run.

Each item is a binary check — it either exists in writing or it doesn't. A verbal assurance is not a check.

01 Timezone & Communication Overlap

■	**Daily overlap is at least 3 hours during YOUR business hours** Insist on this. Partners who call it overlap because 9 pm IST = 3 pm AEST are cheating the clock.	/1
■	**Standups and sprint reviews are scheduled during Melbourne / Sydney working hours** Ask to see a sample sprint calendar, not just a description of their approach.	/1
■	**An escalation contact is reachable in your timezone** Who do you call at 2 pm AEDT on a Wednesday when the build is broken?	/1
■	**Async communication is structured — Loom recordings, documented decisions, written sprint summaries** Verbal-only updates create knowledge silos. Good offshore teams document everything.	/1
■	**Response SLA for urgent issues is defined and contractual** "We respond quickly" is not an SLA. Get a number: e.g., P1 within 2 hours in overlap window.	/1

02 Data Residency & Sovereignty

- ■ **Production data is hosted in an Australian cloud region by default** /1
  AWS ap-southeast-2 (Sydney) or ap-southeast-4 (Melbourne), Azure Australia East, or GCP australia-southeast1.
- ■ **Data never transits through or rests in regions outside your specified boundary without written consent** /1
  Logs, backups, and CI/CD artefacts often end up in US-East by default. Ask specifically about these.
- ■ **The partner can operate inside your cloud account, not only their own** /1
  You retain control. They should be able to deploy into your AWS/Azure org with least-privilege IAM.
- ■ **Offshore team members do not have unlogged access to production data** /1
  Access logs, VPN audit trails, and break-glass procedures should be documented.
- ■ **Data handling agreement (DHA) is in place covering Privacy Act 1988 APP 8 obligations** /1
  The 2024 APP 8 reforms strengthened cross-border accountability — your DHA should reflect current requirements.

03 IP Ownership & Contracts

- ■ **All code, documentation, and design assets vest in you on payment — confirmed in writing** /1
  This should be a standard clause, not a negotiation. Walk away if it is not.
- ■ **The partner executes an IP assignment deed (not just a clause in the SOW)** /1
  In Australian law, a standalone IP assignment deed is cleaner and harder to dispute.
- ■ **There is no reuse clause allowing the partner to reuse your code in other client work** /1
  Common in offshore contracts. Read the definition of "confidential information" carefully.
- ■ **Escrow or source code access is available at contract end** /1
  If the engagement ends, you need to be able to run, maintain, and hand to another team without their help.
- ■ **Non-disclosure obligations cover both the engagement AND the architecture decisions made** /1
  Architecture IP is often overlooked. Your data model, integration patterns, and API design are valuable.

04 Technical Quality & Engineering Process

- ■ **Code is reviewed by a peer before merging — no single-contributor branches to main** /1
  Ask to see a recent PR on GitHub/GitLab. If they hesitate, that tells you something.
- ■ **Automated test coverage is measurable and reported per sprint** /1
  Not just "we do testing" — ask for the coverage metric and the baseline they hold.
- ■ **CI/CD pipeline runs on every PR — not only on release** /1
  Catching regressions late is expensive. Daily deployments to staging should be normal.
- ■ **Dependency vulnerability scanning runs in the pipeline (Snyk, Dependabot, or equivalent)** /1
  OWASP Top 10 A06 — outdated components are still one of the most common exploit vectors.
- ■ **Architecture decisions are documented (ADRs or equivalent) — not just in someone's head** /1
  When the senior engineer leaves, you need to know why the system was designed the way it was.
- ■ **You receive full access to the repository from day one — not at project end** /1
  Visibility is a proxy for trust. Partners who restrict repo access until "delivery" are hiding something.

05 Compliance Readiness

- ■ **Partner has experience with Privacy Act 1988 compliant system design** /1
  Not just awareness — ask for an example of how they handled a consent capture or data deletion request.
- ■ **Infrastructure can be configured to ACSC Essential Eight Maturity Level 1 at minimum** /1
  MFA, application control, patching cadence, and restricted admin access are the baseline asks.
- ■ **Security assessments / penetration tests are available on request (and they have done them)** /1
  An offshore team that has never been pentest'd on a client engagement is a risk.
- ■ **They can work inside your organisation's security tooling (SSO, MDM, VPN, DLP)** /1
  Integrating with your security stack is not optional for enterprise engagements.
- ■ **GDPR-compliant data handling is available if any EU-origin personal data is processed** /1
  Relevant for EUDR compliance, EU-origin supply chain data, or EU-resident customers.

Scoring Guide (27 points total)

Score	Interpretation
23–27 ✓	Strong baseline. Proceed to contract review.
15–22 ✓	Acceptable with gaps. Negotiate missing items before signing.
< 15 ✓	Significant risk exposure. Seek a stronger partner or negotiate hard.

This checklist reflects what we have learned coordinating Melbourne–Delhi delivery across multiple engagements in agritech, sustainability, fintech, and government technology. If you would like to walk through it with a technical team member, book a 30-minute discovery call at brainstacktechnologies.com/contact