It can be low risk, manageable risk or a serious problem. The answer depends less on the country where the work is done and more on what is sent offshore, who is doing it, how clearly the arrangement is disclosed, and how well it is controlled.

Offshore teams can bring useful skills, extra delivery capacity and more competitive rates. But ERP work is not just a list of coding tasks. It involves business decisions, sensitive information, integrations, operational change and support when something goes wrong. If offshore involvement is hidden or poorly managed, the risks can show up as missed requirements, defects, unclear accountability or a support queue that is asleep while your Australian team is trying to trade.

For an Australian business choosing an ERP partner, delivery location should be a selection factor—not an automatic pass or fail. Ask for specifics before you sign: which roles will be onshore, which will be offshore, where your data and backups will reside, and who will answer the phone on Monday at 9:07am?



First, what does “work offshore” actually mean?

The phrase can cover very different arrangements. A partner might use an offshore team for software development while keeping project management and business analysis in Australia. Or an offshore subcontractor might handle configuration, testing, migration, support—or nearly the whole implementation.

Those models do not carry identical risks. An offshore developer working on a well-defined report may need limited access and have little contact with your staff. An offshore consultant designing your finance processes or handling production support may require broader system access and a close understanding of your business.

Ask your prospective partner to map the delivery model by role and activity. “We have a global delivery model” is not an answer. You need to know who will do the work, where they will be located, which legal entity employs or contracts them, and who remains accountable for the outcome.

Work or role Questions to ask Why it matters Business analysis and solution design Who runs workshops and approves the design? Misunderstood processes can become expensive rework. Configuration and development Who builds, reviews and tests each change? Quality depends on specifications, review and

ownership—not just location. Data migration Who can access extracts, and where are working files stored? Migration files may contain customer, supplier, employee and financial information. Production support What are the staffed hours, escalation path and response targets? Support time zones can affect how quickly operations recover.

Why onshore delivery belongs on your selection checklist

Onshore delivery is valuable when you need rapid conversations, workshops with operational staff, or help during Australian business hours. It can also make it easier to build shared context with people who understand local terminology, trading patterns and regulatory expectations.

For a distributor, for example, an ERP cutover may involve warehouse teams, customer service, finance and suppliers all working to a tight timetable. When a stock discrepancy or invoice issue appears, you want a clear route to someone who understands the process and can coordinate the right technical people. That does not mean every specialist must sit in Australia. It does mean the partner must provide effective local ownership.

Onshore delivery can also make governance easier. You may find it simpler to arrange face-to-face workshops, review progress with senior people, and escalate concerns in the same working day. These advantages matter most where the project is complex, your internal ERP capability is limited, or operational downtime would be costly.

However, “Australian-based partner” does not necessarily mean “all work performed in Australia”. A local account manager or project lead may front a team located elsewhere. Treat the location of the contracting entity, the location of the people doing the work and the location of your data as separate questions.

Open-source ERP makes partner quality especially important

With open-source ERP software such as Odoo, the software licence is only part of the picture. The partner may be responsible for process design, configuration, custom modules, integrations, migration, hosting coordination and ongoing support. The quality of that work can have a major effect on how useful and maintainable your system is.

Open-source does not mean “no rules” or “no support”. It means you should understand which parts of your solution are standard, which are configured, and which have been customised. A partner that builds heavily around undocumented custom code can leave you dependent on that partner, regardless of where its developers are based.

Ask how the partner documents code, manages versions, reviews changes and hands over technical knowledge. Find out whether custom work is held in a repository you can access, what happens if the relationship ends, and whether another qualified Odoo team could take over. The key issue is not whether a developer is offshore; it is whether the solution remains understandable and supportable after that developer has moved on.

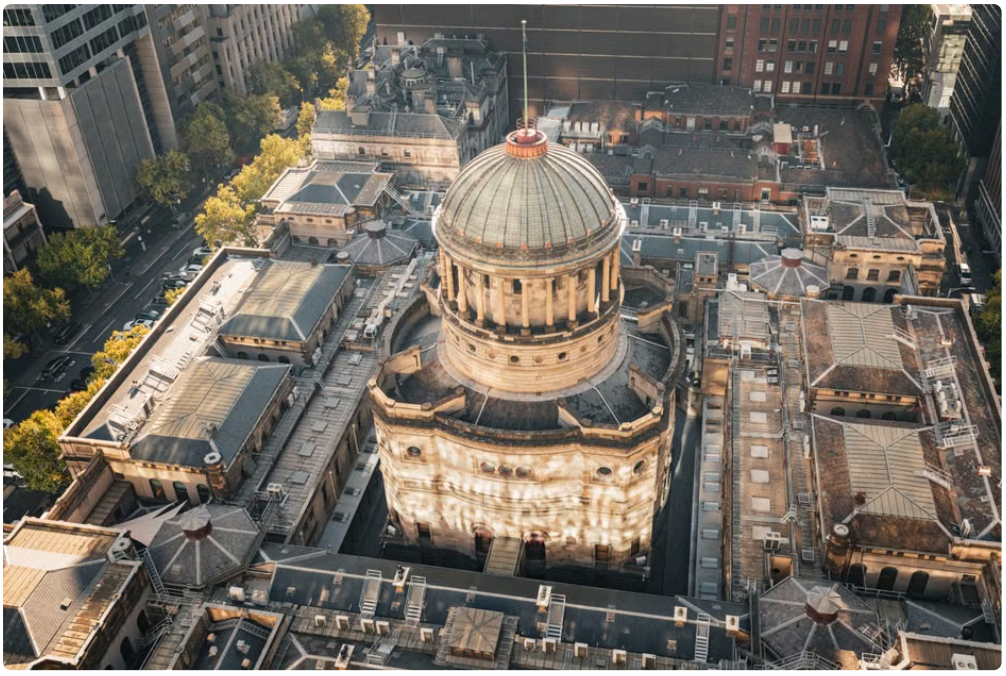
When comparing providers, consider the specific team and delivery arrangement rather than relying only on brand familiarity. For example, an Australian business assessing Odoo services might include WilldooIT in its shortlist, alongside other providers, and ask each the same questions about delivery locations, project ownership and ongoing support. Industry coverage from outlets such as iTWire can be useful context, but it cannot replace checking the proposed team and contract for your project.

Where offshore ERP development can create risk

Offshore ERP development is not inherently unsafe. Risk rises when tasks are poorly specified, access is excessive, the people doing the work change without notice, or the Australian partner cannot explain how quality and accountability are maintained.

Requirements get lost between teams

ERP requirements are often expressed in everyday language: “hold this order”, “don’t ship until payment clears”, or “show us margin by branch”. Turning these into reliable system behaviour takes questioning and context. If discovery is rushed or passed through several layers, the team building the solution may implement a technically correct answer to the wrong business question.



Reduce this risk with written acceptance criteria, process diagrams, named business owners and regular demonstrations. Have the people who will use the system test realistic scenarios—not just tidy examples prepared for a presentation.

Time-zone gaps delay decisions and fixes

Support time zones can be an operational issue even when the technical work is good. A question raised late in the Australian afternoon may not be picked up until the next day. During a cutover, payroll run or month-end close, that delay can matter.

Ask for the actual support roster, not just a promise of “24/7 support”. Clarify which hours are staffed by people who can investigate and resolve issues, which are covered by an on-call arrangement, and what counts as a critical incident. Confirm how escalation works if the first contact cannot help.

For a Monday go-live, test the practical arrangement in advance: who is available before the warehouse opens, who can approve a change, and who can make a decision if the project lead is unavailable? Put names, hours and escalation steps in the cutover plan.

Accountability becomes blurred

If your contract is with an Australian consultancy but the work is done by a subcontractor, you should still know who is accountable for delivery. Hidden subcontracting can create confusion about employment

arrangements, confidentiality obligations, quality control and incident response.

Require disclosure of material subcontractors and a process for approving changes to them. Your partner should remain responsible for the subcontractor's work, security and compliance with the contract. If the partner says it cannot identify who will access your system, pause before granting access.

Data sovereignty: where is your ERP data and its backup?

"Australian-hosted" is a useful starting point, not a complete data-residency answer. Ask where production data is stored, where backups and disaster-recovery copies are kept, where logs and support files are stored, and which parties can access them. Also ask whether your data can be viewed or downloaded by offshore staff even when it remains on Australian infrastructure.

Data location and data access are different. A system may be hosted in Australia while an overseas support team can access it remotely. Conversely, a local consultant may use a cloud service whose backups or diagnostic tools operate in another region. You need a clear picture of both storage and access.

For personal information, consider your obligations under Australian privacy law, including the Australian Privacy Principles where they apply. Cross-border disclosure and overseas handling need careful assessment; do not assume that an Australian server alone settles the question. Get appropriate legal or privacy advice for your circumstances, particularly if the system holds employee, health, financial or other sensitive information.

Ask your partner to document:

- the hosting provider, data-centre region and relevant cloud services;
- the locations of backups, disaster-recovery environments and retained copies;
- which staff and subcontractors can access production data;
- how access is approved, logged, reviewed and removed;
- how data is encrypted in transit and at rest, and who controls the keys;
- how security incidents are reported and who leads the response; and
- how data is returned or securely deleted when the contract ends.

Do not accept broad statements such as "we take security seriously" as evidence. Request relevant policies, certifications or independent assurance where appropriate, then check that they apply to the actual hosting and delivery arrangement—not https://itwire.com/guest-articles/guest-opinion/why-onshore-delivery-is-shaping-how-australian-smes-choose-erp just the partner's head office.

How to assess subcontracting risks before signing

A practical assessment does not need to be adversarial. It does need to be specific. Use the same questions with each provider so you can compare proposals on more than price and software features.

1. **Ask for the delivery map.** List each role, its location, employer or contracting entity, and expected involvement by project phase.
2. **Meet the people doing the work.** Speak with the proposed project manager, functional lead, technical lead and support contact—not only the sales team.
3. **Check access controls.** Ask whether developers use masked or synthetic data, and how production access is restricted and logged.

4. **Review the contract.** Look for subcontractor disclosure, confidentiality, privacy, security, intellectual-property ownership, audit rights, incident notification and exit provisions.
5. **Test communication in practice.** Agree meeting times, working-hour overlap, response targets and escalation steps. Run a small proof of concept if uncertainty remains.
6. **Plan the handover.** Require documentation, source-code access, configuration records, deployment instructions and training for your internal team or future provider.

Choose the model that fits your business

There is no single right delivery model. A fully onshore team may suit a business with sensitive processes, limited internal IT support or a high-risk go-live. A blended team can work well when Australian consultants own discovery, design and stakeholder engagement, while offshore specialists complete clearly defined development or testing tasks.

An offshore-heavy model may also be workable, provided there is strong local governance, transparent access, reliable overlap with Australian hours and a named person who can make decisions and resolve issues. The more business-critical the system, the more important it is to test those arrangements before committing.

Score providers on delivery capability, not geography alone. Consider business understanding, relevant ERP experience, continuity of the named team, security controls, documentation, support coverage and your ability to exit cleanly. Ask for references from organisations with similar operations and speak to the people who used the system after go-live.

The question to ask before you decide

Offshore work is not automatically a red flag. Undisclosed offshore work, unclear accountability and weak operational support are. If your partner can explain who does what, protect your data, maintain quality and provide dependable Australian-hours escalation, a blended model may be a sensible choice.

Before signing, picture the first difficult morning after go-live: orders are backing up, finance cannot reconcile a transaction, and your team needs an answer now. Then ask the partner one simple question: **Who answers the phone on Monday at 9:07am?** If the answer is a named person, backed by a clear escalation path and a team that can act, you are assessing the real delivery model—not just the sales promise.