A lower-cost offshore team can look attractive when an ERP budget is under pressure. But the implementation fee is only one part of the cost. Delays, rework, weak handover, security gaps and support that is unavailable during Australian business hours can quickly erase the saving.

The answer is not that offshore delivery is always risky, or that an Australian provider is automatically better. It is to make delivery arrangements visible, test them before signing, and put practical controls into the contract. For an Australian business implementing Odoo or another ERP, that means looking closely at who does the work, where data is stored, who can access it and who will respond when operations need help.

Use the same question throughout your selection process: **Who answers the phone on Monday at 9:07am?** If the answer is unclear, the support model needs more work.

1. Compare the delivery model, not just the hourly rate

A quote may list an Australian account manager or project lead while assigning configuration, development, testing and support to people elsewhere. That can be a perfectly workable arrangement, but only if it is disclosed and managed. The risk comes when the delivery model changes after you have signed, or when the named local contact cannot make decisions or get a specialist on the line.

Ask each bidder to show who will do each part of the project. Request named roles, locations, expected time commitment and escalation paths. Then ask whether those people are employees, contractors or subcontractors. If subcontracting is allowed, require disclosure and written approval before a new party receives access to your systems or data.

Ask the provider What a useful answer includes Who will deliver each workstream? Named roles, locations, responsibilities and availability—not only a sales contact. Can the delivery team change? Notice, approval rights, replacement standards and a documented handover process. How will decisions be made? A decision owner, agreed response times and a clear route for urgent issues. What happens after go-live? Support hours, severity definitions, escalation contacts and coverage for Australian working hours.

Onshore delivery is a valid selection factor, particularly for workshops, warehouse observation, payroll cutovers and complex process decisions. A local consultant can visit a site, hear how work actually happens and resolve questions without waiting for another time zone. That does not mean every task must be performed in Australia. It does mean you should understand which tasks benefit from local presence and who owns them.

When comparing providers, look beyond claims such as “global delivery model”. Ask for specifics: which city or country each team works from, how many hours overlap with your team, and whether the provider has Australian staff available for critical milestones. Australian ERP coverage in publications such as iTWire can help businesses understand the local technology landscape, but vendor selection still depends on checking the proposed team and contract for your own project.

2. Treat Odoo’s flexibility as a reason to check partner capability

Open-source ERP gives businesses room to inspect, adapt and extend software. That flexibility can be valuable, but it also increases the importance of choosing a capable implementation partner. The software does not decide how your chart of accounts is designed, whether your warehouse processes make sense, or whether a custom module will be maintainable after the original developer leaves.

With Odoo, the implementation partner's choices can shape the long-term cost of upgrades and support. Ask which requirements will be handled through standard configuration, which require custom development and which can be addressed by changing the business process. A partner that proposes custom code for every difference may leave you with avoidable technical debt.

Check the work behind the proposal

- **Reference projects:** Ask for examples in a comparable industry, with similar transaction volumes, locations or manufacturing complexity.
- **Technical ownership:** Identify who reviews code, tests changes and documents customisations.
- **Upgrade approach:** Ask how custom modules will be assessed and tested when you upgrade Odoo.
- **Knowledge transfer:** Confirm that your staff will receive configuration records, process documentation and administrator training.
- **Exit options:** Establish that you can obtain your data, code and relevant documentation if you change providers.

For example, a business considering WilldooIT should assess the specific team and scope proposed for its needs, just as it should with any Odoo partner. Do not rely on a brand name, partner status or presentation alone. Ask who will configure your system, who will review the work and who will provide ongoing help.

3. Make hidden offshore work visible before signing

"Hidden offshore work" is not simply work completed overseas. It is work performed by people whose location, role or access was not disclosed clearly enough for you to assess the consequences. That can create gaps in communication, accountability, security and support—especially when a critical issue lands outside the team's working hours.

Build a delivery schedule into the statement of work. It should identify workstreams, owners, locations, dependencies, customer responsibilities and acceptance criteria. If a provider intends to use offshore developers or testers, have it state that explicitly and explain how work will be reviewed before release.

Put practical controls in the contract

1. **Require disclosure.** List the provider's delivery locations and subcontractors, and require advance written approval for material changes.
2. **Define acceptance.** Specify what "done" means for each milestone, including test evidence and business sign-off.
3. **Control scope changes.** Require an estimate, impact assessment and approval before extra work begins.
4. **Protect continuity.** Require documented handover, current configuration records and transition assistance if key staff leave.
5. **Make escalation real.** Name the person who can make a decision when the project lead is unavailable.

Keep a risk register from the start. Record each risk, its owner, likelihood, impact, mitigation and trigger for action. For example, if a key developer is available only during a narrow overlap window, the mitigation might be a local technical lead, peer-reviewed documentation and an agreed escalation route.

Do not use low hourly rates as a substitute for a total-cost comparison. Include discovery, data cleansing, integration work, testing, travel, post-go-live support, upgrades and the internal time your staff must

contribute. A cheaper proposal with unclear assumptions may end up costing more because your team has itwire to explain processes repeatedly or repair incomplete work.

4. Set an SLA that works in Australian time

“Support available” is too vague to protect an operating business. Your service-level agreement (SLA) should state the support channel, coverage hours, response targets, escalation steps and what happens when the first contact cannot resolve the issue. It should also explain how severity is assessed.

Pay particular attention to **SLA and support hours**. If your warehouse starts at 6am, or payroll and dispatch have fixed deadlines, standard office hours may not be enough. Match coverage to your real operating calendar rather than accepting a generic support window.

SLA item Questions to settle Coverage Which Australian time zone applies? Are public holidays, early starts and month-end periods covered? Severity What counts as a business-critical outage versus a workaround or minor defect? Response and restoration Are targets for acknowledgement only, or do they include updates, workaround and restoration efforts? Escalation Who can be contacted if the service desk does not respond or the issue worsens? Release support Who is available during deployments, data loads and the first days after go-live?

Test the support path before go-live. Ask the provider to walk through a realistic incident, such as orders failing to sync with an integration or warehouse users being unable to complete picking. Confirm what information your staff should provide, where tickets are logged and how they can reach a person if the portal is unavailable.

Also plan the cutover around the people who will use the system. A Monday morning payroll or dispatch change is not a good time to discover that the only person who understands the migration is asleep in another time zone. Agree a named go-live roster, on-call contacts and decision authority in advance.

5. Specify data sovereignty, hosting and access restrictions

“Australian-hosted” is important, but it is not a complete data-security answer. Confirm where the production database, file storage, backups, logs and disaster-recovery copies are located. Ask whether support staff in other countries can access the system or export data, even if the primary hosting environment is in Australia.

Data sovereignty and privacy obligations depend on the information involved, your industry and the arrangements you have with customers and suppliers. Get advice appropriate to your circumstances rather than assuming that a local hosting region resolves every issue. Make the provider describe its architecture in writing, including backup locations, retention periods, recovery objectives and how data is securely deleted at the end of the contract.

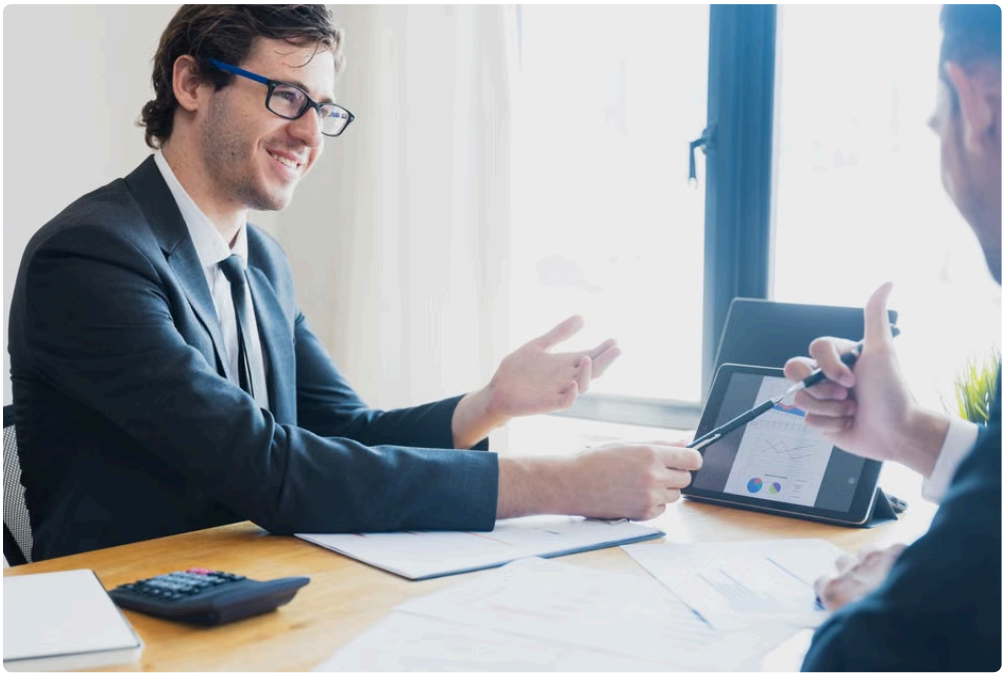
Use access restrictions that match the work

- Give each person a named account; prohibit shared administrator logins.
- Use least-privilege permissions, with elevated access approved and time-limited.
- Require multi-factor authentication and secure remote access.
- Restrict access by role, environment and, where practical, approved location or network.
- Log administrative activity and review access regularly, especially when project staff change.

- Use masked or synthetic data for development and testing wherever feasible.
- Set a process for revoking access promptly when a person leaves the project.

Ask who can access production data, for what purpose and with whose approval. Confirm how support staff handle screenshots, database extracts and diagnostic files. A vague assurance that data is “secure” is not enough; you need controls that can be explained, checked and reflected in the contract.





6. Reduce implementation risk with staged proof

Do not wait until the full system is built to find out whether the team understands your business. Start with a discovery phase that produces process maps, a data assessment, integration inventory, solution design and delivery plan. Make the outputs useful to your business, not just internal project documents.

Then validate the riskiest assumptions early. Run a representative data migration. Test a real order-to-cash or procure-to-pay scenario. Confirm that the system handles your product variants, warehouse locations,

tax treatment and reporting needs. For manufacturers, test a realistic bill of materials and production process before committing to a large custom build.

Use stage gates. Move from discovery to build, and from testing to go-live, only when agreed evidence is available. That evidence might include reconciled opening balances, passed user acceptance tests, completed training and signed-off support arrangements. If a gate is missed, agree the corrective action rather than letting the schedule hide the problem.

A practical selection checklist

- Have we seen the actual delivery team, including locations and subcontractors?
- Is onshore availability defined for workshops, cutover and urgent decisions?
- Does the proposal distinguish standard Odoo configuration from custom development?
- Are code, documentation, data and exit assistance addressed in the contract?
- Do SLA and support hours match our Australian operating hours and critical periods?
- Are hosting, backup and disaster-recovery locations documented?
- Are access restrictions, logging and offboarding controls clear?
- Have we tested a migration and business-critical workflow before full rollout?

Conclusion

A cheaper offshore team can be a sound choice when the work is transparent, the team is capable and the controls fit your business. Reduce risk by selecting on delivery capability as well as price, making offshore participation explicit, and setting enforceable expectations for support, security and handover.

For open-source ERP such as Odoo, partner quality matters because implementation decisions become part of your operating environment. Confirm where your data and backups live, apply sensible access restrictions and test support before the first live transaction. Most importantly, make sure the person answering at 9:07am on Monday can actually help your Australian team keep trading.