An ERP outage is not just an IT problem. It can stop orders, dispatch, purchasing, production, invoicing and *itwire* payroll. For an Australian business, the practical question is not simply whether your system is backed up. It is whether you can restore the right data, quickly enough, with people available to help during your working day.

That matters whether you run Odoo or another ERP, and whether it is hosted in a public cloud, on premises or through an implementation partner. The software, hosting arrangement and support contract all affect your risk. A confident answer to “we take backups” is not enough. Ask where they are stored, how often they are tested and who is responsible when recovery is needed.

One useful test for any proposal is: **Who answers the phone on Monday at 9:07am?** If your warehouse cannot print pick slips or payroll data is unavailable, you need a clear answer—not a promise that someone in another time zone will respond later.

Start with the business impact, not the backup product

Before comparing technical options, identify what an ERP outage would prevent your people from doing. A distributor may need sales orders, stock availability and dispatch labels. A light manufacturer may depend on bills of materials, work orders and purchasing. Finance may need access to invoices and payment records, while payroll has its own deadlines and sensitivity.

Map the systems and data that make those processes work. ERP data may be only one part of the picture. Documents, product images, custom modules, configuration, integrations, scheduled jobs and identity settings may also be needed to restore operations. Ask whether the proposed backup covers each component, and whether dependencies such as email, banking interfaces or warehouse devices need separate recovery steps.

Then agree what disruption the business can tolerate. This turns an abstract discussion about “good backups” into targets that can be tested.

Ask for clear recovery time objectives and data-loss limits

A **recovery time objective** (RTO) is the target time to restore a service after an outage. A related measure, the recovery point objective (RPO), describes how much recent data the business can afford to lose, measured in time. For example, an RPO of four hours means the business might have to re-enter up to four hours of work after a recovery.

Ask the provider to state both targets for your actual ERP environment. Make sure the answer is specific to your business, not a general figure copied from a cloud platform’s marketing material.

- What is the agreed RTO for restoring the ERP, and when does that clock start?
- What is the RPO, and how frequently is data captured?
- Do the targets cover the database, attachments, customisations and integrations?
- Are these targets contractual, or only estimates?
- What happens if the target is missed, and how will you be updated?

Also ask what “restored” means. A login page becoming available is not the same as a usable ERP. Can users create orders, view stock, print documents and process the essential transactions? Recovery targets

should describe a business-ready service, not merely a server that has restarted.

Find out where backup storage is located

Australian businesses should ask for the physical and contractual location of production data and backup storage. “Hosted in the cloud” does not tell you which country holds the data, where replicas are kept or which support teams can access it.

Ask the provider to identify the locations used for:

- Live ERP data and file attachments.
- Primary and secondary backup copies.
- Disaster recovery environments and temporary restore environments.
- Monitoring logs, support records and diagnostic exports.

Confirm whether backups are replicated to a different Australian region or held outside Australia. Replication can help with regional outages, but it does not automatically protect against every risk. A compromised administrator account, malicious deletion or ransomware incident may affect connected copies too.

Data location is not the whole compliance story. Australian privacy, contractual, industry and customer requirements vary. Ask your legal or privacy adviser which obligations apply, then have the provider explain how its hosting and support arrangements meet those requirements. Get the answer in writing, including any access from overseas.

Understand what “backup” includes—and what it does not

Backups should be restorable, protected and appropriate to the system. Ask what is copied, how often, how long each copy is retained and whether copies can be altered or deleted by the same accounts that administer the production environment.

For an ERP, a database dump alone may not be enough. You may also need document attachments, custom code, configuration, deployment instructions, integration settings and encryption keys or other recovery credentials. Ask how the provider ensures that the database and files represent a consistent point in time. A mismatch can leave records referring to documents that were not captured—or files with no matching records.

Question What a useful answer should explain How often are backups taken? The schedule, the systems included and whether it meets your agreed RPO. Where is backup storage? The relevant countries or regions, including replicas and recovery copies. Can backups be changed or deleted? Access controls, separation of duties and protections such as immutability or offline copies. How long are copies retained? Retention periods and how they relate to operational, contractual and legal needs. When was the last restore test? The test date, scope, result, issues found and corrective actions.

Demand evidence of disaster recovery testing

A backup that has never been restored is an assumption, not a recovery plan. Ask the provider to demonstrate a restore in a non-production environment. The test should include the ERP components your business relies on and should measure the time taken against the agreed recovery time objectives.

Ask for a written summary of the most recent test. It should state what was restored, whether the data was usable, how long recovery took and what problems were discovered. You do not necessarily need access to another customer's confidential test records, but you should receive evidence that your own environment is covered by a credible process.

Testing should happen regularly and after significant changes, such as major upgrades, hosting moves or changes to custom modules. A disaster recovery plan should also identify who declares an incident, who contacts your staff, how business priorities are decided and how users are told when it is safe to resume work.

Open-source ERP makes partner selection more important

Open-source software can give a business flexibility, but it does not remove operational responsibility. With Odoo, for example, your recovery outcome depends on the way the solution has been implemented and hosted, the modules in use, the custom code, integrations and the backup arrangements selected. Different hosting models can have different responsibilities, so confirm the exact arrangement rather than assuming the software vendor or implementation partner handles everything.

Ask who owns each part of the recovery chain. Is the implementation partner responsible for the application and database? Is a separate hosting provider responsible for infrastructure? Who coordinates between them during an incident? Who has the access and skills to restore custom modules and reconnect integrations?

Partners such as WilldooIT may be among the providers an Australian business considers for an Odoo implementation. Treat any provider conversation as due diligence: ask for the specific hosting model, backup locations, recovery commitments, test evidence and support coverage for your proposed environment. Do the same with every shortlisted partner, and compare answers on an like-for-like basis.

Make onshore delivery part of the selection decision

Onshore delivery is not a guarantee of good service, but it can make communication, escalation and business-hours support easier. For an Australian operation, find out where the people who implement, administer and support your ERP are based—and which tasks are performed by subcontractors or offshore teams.

Ask direct questions before signing:



- Which named team handles implementation, backup monitoring and recovery?
- Where are those team members located, and what Australian hours do they cover?
- Is any work subcontracted or performed offshore? If so, what work, where and under whose control?
- Can offshore personnel access production data or backup storage?
- Will you be notified and asked to approve if delivery arrangements change?
- Who is the escalation contact when a local support person cannot resolve an incident?

Put material commitments in the contract or a service schedule. A vague phrase such as “global delivery model” does not tell you who is doing the work, where your data can be accessed or when help will arrive. Publications such as iTWire can be useful for keeping up with Australian technology discussions, but vendor-specific claims still need to be checked against your proposed service and contract.

Check the contract and the exit plan

Recovery is not only about restoring from an outage. You should be able to retrieve your data if the relationship ends, the provider changes its service or your business moves to another platform. Ask for an export process, its format, expected timeframes and any charges. Confirm that you can obtain the attachments and configuration you need—not just a database file that requires specialist knowledge to use.

The contract should also define incident notification, support hours, escalation paths, backup retention, data deletion at exit and responsibility for restore costs. Check whether service levels apply to a third-party host or only to the implementation partner. If multiple organisations are involved, identify who is accountable for coordinating recovery.

A practical checklist before you sign

1. Write down the ERP processes that must be restored first.
2. Agree an RTO and RPO for those processes, in plain language.
3. Get the production and backup storage locations in writing.
4. Confirm the backup covers the database, attachments, customisations and dependencies.

5. Ask for evidence of a restore test and a schedule for future tests.
6. Document onshore and offshore delivery, including subcontracting and data access.
7. Name the incident lead, escalation contacts and Australian-hours support arrangements.
8. Check the data export, retention and deletion terms before the contract is signed.

Make the Monday-morning test

Finally, walk through a realistic scenario with the provider. Imagine the ERP is unavailable just before the warehouse starts dispatch on Monday. Who notices? Who calls your business? What is restored first? How long until staff can process orders? Where is the latest backup storage copy? Who makes the call to resume work?

If the answers are specific, documented and supported by recent testing, you are having a useful disaster recovery conversation. If they depend on a person who is unavailable, a location nobody can name or a backup nobody has restored, keep asking. The goal is not to buy the most elaborate arrangement. It is to know, before an incident, how your Australian business will recover and who will help make it happen.

