



The 30-Point Offshore Due Diligence Checklist

A photograph of three business professionals (two men and one woman) smiling and looking at a laptop. The man on the left is holding a smartphone. They are standing behind a wooden podium. The image is framed within a large, light blue circle on a dark blue background.

**A PRACTICAL FRAMEWORK TO REDUCE LEGAL
SECURITY, AND OPERATIONAL RISK**

Table of Contents

The 30-Point Offshore Due Diligence Checklist

Why Due Diligence Matters in Offshore Hiring	3
The Legal & Employment Risk Checklist	7
The Information Security Checklist	11
The Operational Visibility Checklist	15
Red Flags to Watch For	16
PeoplePartners: Your Compliance Shield	17



Why Due Diligence Matters in Offshore Hiring

As global teams become the norm, businesses are discovering that the real risks of offshore hiring aren't always about productivity. Regulators and industry research consistently show that the biggest risks in offshoring come from governance, security, and compliance gaps rather than talent quality.

Recent industry data shows:



- 45% of multinational companies report compliance issues when expanding global teams according to Deloitte's Global Payroll Benchmarking Survey.
- Over a third of data breaches now originate from third-party vendors or partners, underscoring the growing risk introduced by outsourced or distributed teams.



- Weak supervision of offshore operations increases operational and cyber risk. Regulators note that risk increases when outsourced functions are not adequately supervised or monitored, particularly when those functions are performed internationally.
- Many organizations lack formal frameworks to manage offshore providers. Regulatory reviews found that some companies relying on offshore teams had no structured policies, due diligence processes, or monitoring frameworks in place.

The challenge isn't whether offshore staffing works. It's whether the structure behind it is built correctly.

This checklist helps you assess whether your offshore setup protects your business before small gaps become large liabilities.

If you can confidently answer “**Yes**” to these 30 points, you likely have a **secure offshore framework**. If not, you may be carrying risks you didn't intend to take on.

Legal & Employment Risk

Hiring staff in another country introduces local labor law, tax, and employment compliance requirements that many companies underestimate.

Without the right structure, businesses risk:

- Worker misclassification
- Payroll tax violations
- Permanent establishment tax exposure
- Unenforceable contracts
- Intellectual property disputes



Legal & Employment Risk

For example, regulators in Australia recently highlighted cases where offshore workers were reclassified as employees, increasing compliance scrutiny for companies using contractor structures.

One solution many global companies use is an **Employer of Record (EOR)**.

An EOR legally employs offshore staff on your behalf while you manage their day-to-day work.

This allows businesses to access global talent while maintaining compliance with local labor laws, payroll obligations, and employment protections.

Legal & Employment Risk Checklist

- ☐ Is there a legal entity employing your offshore staff?
- ☐ Does your provider act as an Employer of Record (EOR)?
- ☐ Are employment contracts compliant with local labor law?
- ☐ Who manages statutory benefits and payroll tax?
- ☐ Who carries liability in a workplace dispute?
- ☐ Are termination processes legally structured?
- ☐ Are IP ownership clauses clearly defined?
- ☐ Are confidentiality agreements enforceable locally?
- ☐ Are you protected from co-employment risk?
- ☐ Is there documented HR governance?

Explainer

What is an Employer of Record (EOR)?

An Employer of Record is a company that legally employs staff on behalf of another organization in a specific country.

The EOR becomes responsible for:

- Employment contracts
- Payroll and statutory taxes
- Mandatory benefits
- Labor law compliance
- Termination processes



This structure significantly reduces the legal risk of hiring in jurisdictions where your company does not have an entity.

Information Security & ISO Standards

When offshore teams access your systems, they are often working with:

- customer data
- financial information
- proprietary intellectual property
- internal systems

Without strong security frameworks, this creates serious exposure.

High-quality offshore providers typically adopt international information security standards.



Information Security & ISO Standards

The most recognized is **ISO 27001**, developed by the **International Organization for Standardization (ISO)**.

ISO 27001 defines how organisations must build and maintain an **Information Security Management System (ISMS)** to protect sensitive data through policies, access controls, monitoring, and continuous audits.

This certification signals that security processes are documented, audited, and continuously improved.

Information Security Checklist

- ☐ Is your provider ISO certified?
- ☐ Which ISO standard do they hold (e.g., ISO 27001)?
- ☐ Is there a documented information security management system?
- ☐ Are devices company-issued and secured?
- ☐ Is multi-factor authentication enforced?
- ☐ Is access role-based and restricted?
- ☐ Is data activity logged and auditable?
- ☐ Are employees trained in data security?
- ☐ Is there a breach response protocol?
- ☐ Are client systems accessed via secure environments?

Why This Matters

Weak security controls in outsourced environments can expose businesses to:

- intellectual property theft
- data breaches
- regulatory penalties
- reputational damage



A major cyberattack against outsourcing provider Capita exposed personal data of approximately 6.6 million individuals and cost the company over £25 million in recovery and remediation.

Security frameworks are not a “nice to have”.

They are a **business continuity requirement**.

Operational Visibility & Productivity

One of the biggest frustrations companies experience with offshore teams is lack of visibility. Not because teams aren't working, but because performance systems were never designed for distributed workforces.

Visibility protects margin.

Guesswork erodes it.



Operational Visibility & Productivity

Regulators reviewing offshore outsourcing arrangements have repeatedly found businesses relying on informal oversight with little documented governance or monitoring.

Without visibility, companies struggle to answer simple questions:

- Are roles clearly defined?
- Are KPIs being met?
- Are workflows documented?
- Are managers accountable?

The result is margin leakage and productivity uncertainty.

Operational Visibility Checklist

- ☐ Do you have defined KPIs per role?
- ☐ Is productivity tracked transparently?
- ☐ Are activity logs available if required?
- ☐ Do you receive performance reporting?
- ☐ Is there structured team oversight?
- ☐ Are workflows documented?
- ☐ Is output reviewed regularly?
- ☐ Are performance improvement processes in place?
- ☐ Is there local leadership managing staff?
- ☐ Do you have margin visibility per role?

Red Flags to Watch For

If you answered “No” to more than 5 items, your offshore setup may carry hidden risks.

Common exposures include:

Legal Exposure

Unclear employment structures can create liability for payroll tax, worker misclassification, or employment disputes.

Data Security Risk

Weak security frameworks increase the likelihood of breaches involving international teams and vendors.

Margin Leakage

Poor visibility into productivity and workflow management can erode the financial benefits of offshore staffing.

Brand Vulnerability

Security failures or employment disputes in offshore operations can damage customer trust and reputation.

Offshore staffing works best when compliance, security, and visibility are designed into the model from the beginning.

PeoplePartners Is Your Compliance Shield

If this guide surfaced questions, that's normal. Offshore due diligence gets complicated fast when you try to piece the setup together across multiple moving parts. PeoplePartners simplifies that by providing offshore staffing with the key safeguards built in from day one:

ISO-Certified Information Security

ISO/IEC 27001:2022 certified, with documented security practices and controls to help protect client data across systems, access, and handling.

Employer Of Record (EOR) Structure

Employer of Record structure, with payroll, statutory obligations, and local employer requirements handled in-country to support proper offshore employment setup.

Structured Productivity Monitoring

Productivity monitoring with screen, application, and idle tracking to improve work visibility and protect your staffing investment as you scale.

From Due Diligence To A Decision

You came here for one thing: confidence that your offshore plan is set up the right way. Offshore staffing is rarely complicated because of talent. It gets complicated when the setup underneath the team isn't defined early enough.

This checklist gives you the lens. The next step is making it real for your team. If you want to move forward with clarity, you'll want to translate this into three practical decisions:

- What you're trying to achieve
- The roles that make sense
- The structure that will hold as you scale

A short consultation with PeoplePartners is the simplest way to turn this into a clear offshore staffing plan.



Speak with one of our Workforce Specialists Today.

In a Free Consultation, we'll discuss your goals and current setup, then outline how an offshore team could be structured to support your operations as you grow.

This Is A Good Fit If You're:

- Planning your first offshore hire and want to get the setup right
- Scaling an existing offshore team and want the structure to hold
- Unsure about the right roles, ramp, or team design
- Looking for a staffing partner that can support the setup, not just fill seats

BOOK A CONSULTATION

