THE SCALERS

Offshore IT project security: strategies to stay safe

Introduction

Offshoring software development has become a major global trend in recent years that is expected to continue rising in popularity.

It allows companies to leverage **highly skilled** and **cost-effective developers** from overseas and enables them to focus their efforts on core business activities. However, it also comes with potential risks that must be properly managed.

So, let's take a closer look!

Types of project development risks

To effectively manage offshore IT project risks, it’s crucial to identify risks in 4 key areas:

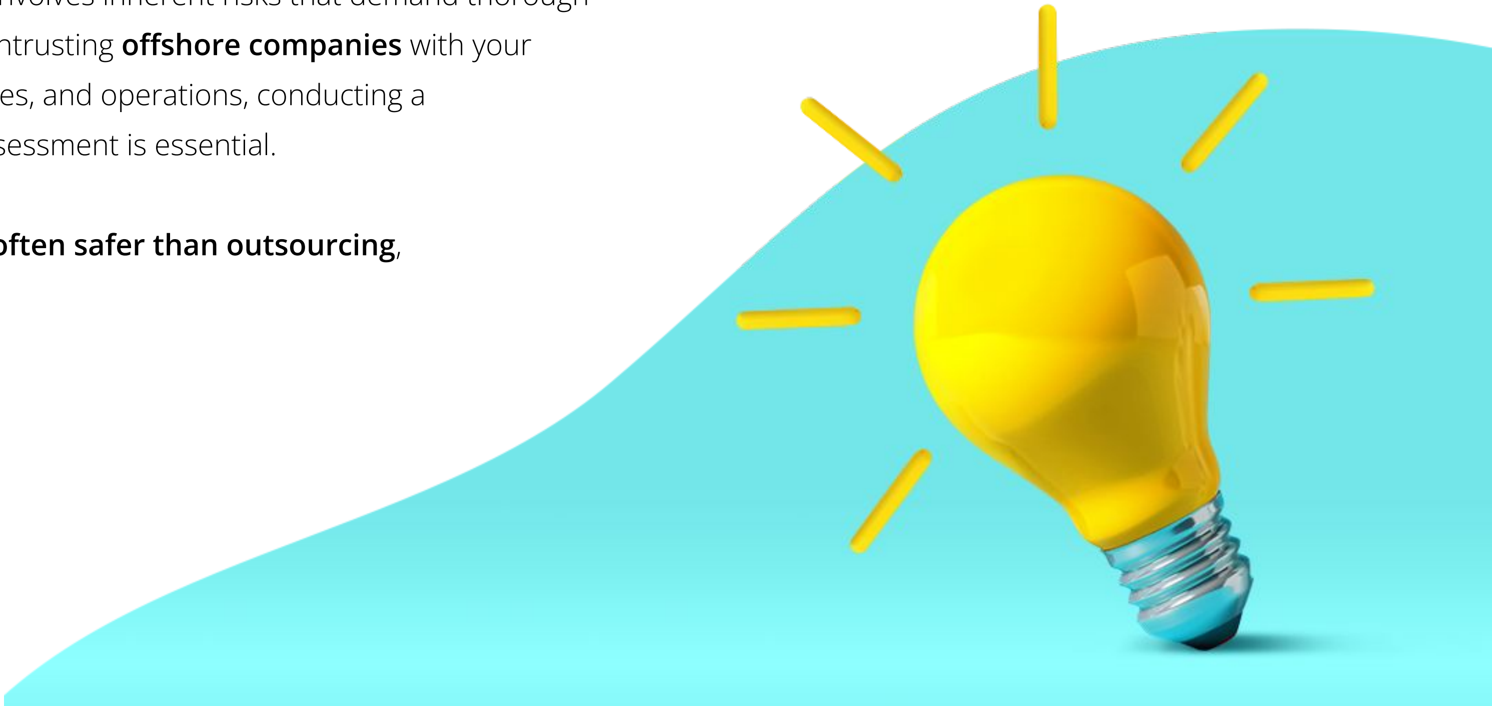
- **Organisational**
- **Scheduling**
- **Operational**
- **Technological**

Knowing these hurdles allows assessing the project's strengths, weaknesses, threats, and opportunities.

Top risks to be aware of in offshoring IT projects

Offshoring IT projects involves inherent risks that demand thorough consideration. When entrusting **offshore companies** with your business data, processes, and operations, conducting a comprehensive risk assessment is essential.

Though **offshoring is often safer than outsourcing**, it's still not risk-free.



Lack of transparency and communication

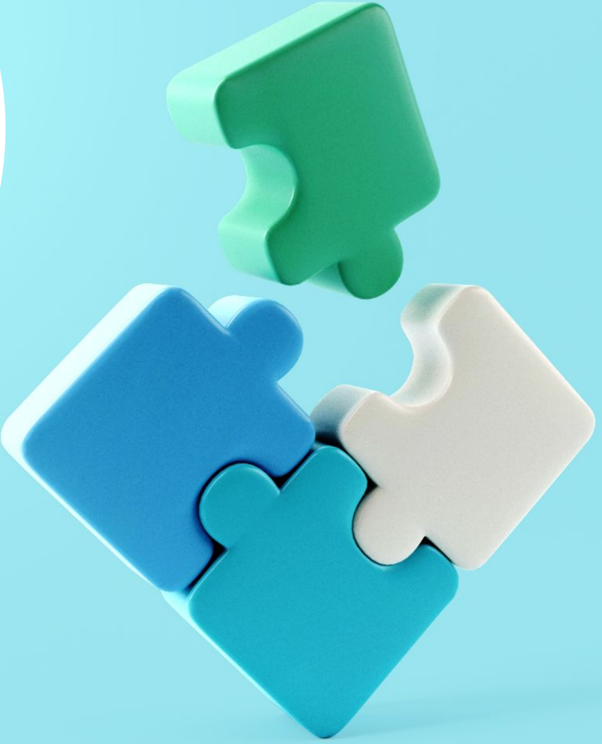
In offshore IT projects, a lack of transparency can lead to **cost escalation** and **delivery delays**. However, compared to traditional outsourcing, **offshoring typically offers better visibility**.

To mitigate this risk effectively, it's important to maintain open and two-way communication throughout the project lifecycle.

Gaps in project planning and alignment

A limitation of proper project planning and alignment can make **offshoring software development** more challenging. Working with an experienced offshore partner is the best strategy to avoid project mishaps.

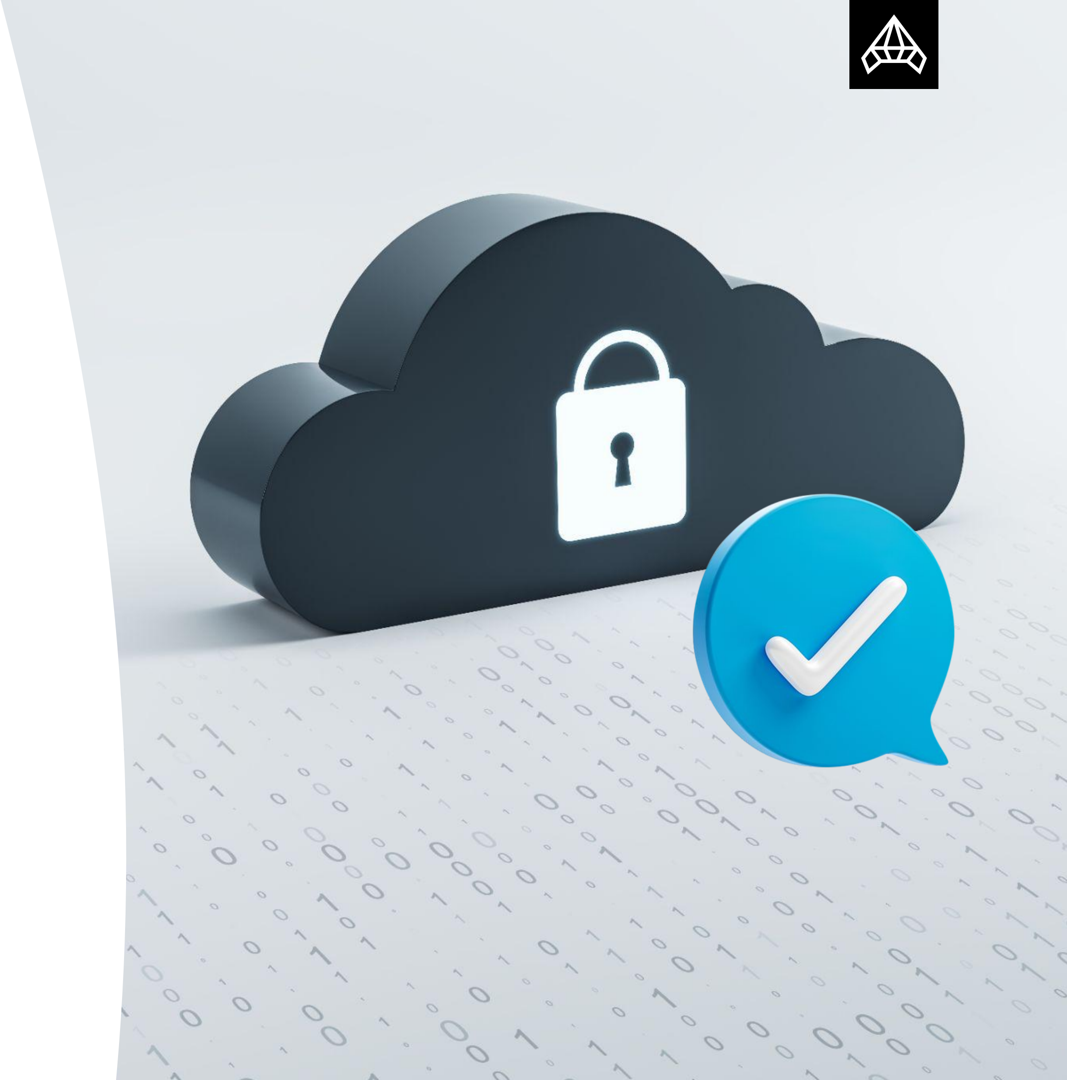
When you adopt well-thought-out strategies and efficient **project management**, it not only reduces risks but also makes the whole process smoother.



Data security and privacy risks

Weak data security is a significant offshoring risk, with **68% of organisations** expressing concerns. Varying data regulations across countries can also cause issues.

Offshore partners get access to critical data, so poor cybersecurity makes data vulnerable to attacks, undermining the business. Ensuring adequate security, like **ISO 27001 certification,** is a must to guard sensitive data and digital assets when offshoring.



Timezone and cultural communication challenges

Offshore locations often introduce t**ime zone variations** and **cultural differences**. These can result in delayed responses that impact project timelines. Additionally, cultural differences may lead to misunderstandings and frustration, ultimately reducing productivity.

To avoid these situations from hapenning, it's crucial to establish alignment through a partner who can facilitate effective communication. Such partnerships play a critical role in ensuring **seamless collaboration and project success**.

Securing offshore IT projects: Key tips

1. Choose the right **offshore partner** that fits your culture to bridge gaps and enable collaboration.

2. Adopt the **best cooperation model** and allow time for synchronisation and communication between teams.

3. Prioritise **data security risks** - identify, evaluate, and mitigate with appropriate strategies.

4. Consider spending on security measures - **55% of businesses** are increasing data security budgets.

Wrapping up

While offshoring offers many benefits, it's important to recognise that it comes with certain risks. Fortunately, these risks can be minimised by **teaming up with a seasoned offshore partner** and putting the right security measures and tools in place.

Successful offshoring of IT projects hinges on thorough planning and diligent vetting. By **collaborating with professionals** who grasp both the technical and cultural aspects, you can pave the way for successful global teamwork and project completion.

Thank you

THE SCALERS®

thescalers.com