



Managing Political Risk in Offshore Outsourcing

Randy Kirihara has a background in information technology product/services sales, vendor management and offshore software development. He is actively involved in offshore program management at a fortune 500 corporation. Offshore software development has been growing rapidly over the past several years. Randy believes that a disciplined and coordinated approach is essential to realize the potential benefits of offshore development.

Since the mid-1990's, the Indian offshore software services outsourcing industry has significantly outperformed most other segments of the IT industry. Even in the post-9/11 world, this industry continues to grow, although at a slightly less frenzied pace.

Long standing customers of these services are well aware of general risks of doing business in India, most of which are related to inadequate infrastructure. To create the necessary environment in which to conduct business, Indian software services vendors have been forced to implement their own infrastructure, reducing their dependence on public services. This has resulted in self-contained work campuses with private services such as power backup, satellite communications, water purification and transportation systems.

The presence of these in-house capabilities effectively mitigates the most commonly perceived general risks of doing business in India. Customers could be assured that work would continue relatively disruption free, encouraging them to migrate mission critical work to India.

New Awareness of Political Risk

But the post-9/11 world and most recently, escalation of the India/Pakistan Kashmiri conflict has created a heightened awareness of political risks of doing business in India. These events are causing western companies to consider potential impacts of catastrophic terrorist attacks and acts of war on their work occurring in India. Although many offshore vendors will have their own business continuation plans, such plans may not adequately address political risk.

Before developing a contingency plan to manage political risks, companies should consider the nature of the offshore work being performed. Factors that will influence the type of contingency plan needed include the onsite/offshore staffing ratio, the complexity of the work being performed at the offshore location and the business impact of interrupted service.

An act of war or terrorism could result in any number of consequences that effectively shut down an offshore development center for an indefinite basis. This includes destroyed or damaged work facilities, infrastructure damage (water, power, communications, transportation) or loss of life. A vendor contingency plan assuring the continuation of offshore work following such a major catastrophe is highly unlikely.

Vendor Business Continuation Plans

Most offshore vendors will have a business continuation plan. But it is beneficial to analyze such plans, identify shortcomings and to develop your own plan to fill major gaps. Vendor plans will typically include redundant communication links, nearby spare facilities and possibly facilities located in other countries. But in a massive catastrophe, as can happen in war, it is

unlikely that these plans will allow vendors to take care of all of their customers at expected service levels. Potential client impacts include longer project completion dates, higher than anticipated costs and loss of critical knowledge, skills and experience that could jeopardize the success of the project. For these reasons, it is prudent to develop your own plan to migrate work away from the geography in question should a catastrophe beyond the scope of the vendor's business continuation plan occur.

It is common for an offshore vendor to have multiple communication links flowing in and out of an offshore development center. But should a catastrophic event occur, what assurance is there of the continued availability of these links? If only one link is operational, will the vendor be able to service all of its customers? And if the facility is severely damaged or if life is endangered, will workers be available or willing to report to work?

Vendors may count on nearby underutilized facilities that could be occupied in an emergency. All well and good, but some of these facilities are probably dangerously close to the main facility or may be located in a similarly at risk location. Some vendors' main facilities contain hundreds or thousands of people. It would be prohibitively expensive to build and maintain a fully equivalent backup facility. It wouldn't be prudent to assume that your operations would continue as today in the event of catastrophe.

A third major component of vendor business continuation plans is a geographically remote development center, often in another country. If a catastrophe occurred at a development center in New Delhi, it might be possible to shift the employees that normally work in this center to the remote development center. But since we are talking about people with personal goals, families and complex behavior, you shouldn't assume this will be easy to accomplish. You can't control these people nor can you control government immigration policies or processes that may limit movement. For these reasons, movement of personnel should be viewed as a bonus rather than a core contingency strategy.

A fourth option could be to move work, not people, from the imperiled facility to an unaffected vendor facility in a different country. The ability to do so must be balanced against project management and processes utilized by both vendor and client. People dependency is common and it may be less painful or lower risk to simply move work back onsite rather than allow the vendor to move the work on a wholesale basis to an entirely new facility.

Cost Impact

Services contracts typically contain a "force majeure" clause that releases the vendor from the obligation of providing services when impacted by an "act of god" or war. So even if the vendor is willing to execute a business continuation action, such as moving personnel to a third location, who would bear the costs of doing so? The vendor may not be willing to move personnel without additional compensation from the client. And force majeure could release the vendor from obligation of performing the service.

Client Business Continuation Planning

The nature of your offshore projects will influence the type of contingency plan to be adopted. Many projects may not be able to tolerate prolonged or indefinite outages. Such projects should have a healthy onsite staffing ratio (most offshore projects are executed with a combination of onsite and offshore resources). This will allow you to shift work onsite if needed. It may not be possible to perform at the same service level or low cost, but having the capability to quickly move work between locations is a powerful contingency factor.

To be able to shift work to onsite resources, you must ensure their normal workload is not fully mission critical. This will allow you to suspend or transfer part of their normal workload,

which will be exchanged for higher priority work being transferred from the disabled offshore facility.

Projects with a substantial ratio of offshore to onsite resources (such as 80% offshore/20% onsite) are more vulnerable to prolonged outages. It would be a rare situation for such a heavily leveraged project to be minimally impacted from a prolonged outage. Don't put all heavy offshore leveraged projects in a single location - it would be prudent to spread such projects among multiple geographic sites.

Actions Within Client Control

Offshore vendor business continuation plans are beneficial to manage general risks but may not be sufficient to meet prolonged and widespread outages that could be expected from acts of war or terrorism. Clients can anticipate project delays, increased costs and in extreme cases, cancelled projects should a catastrophe impact a remote development center. Clients can't control acts of hostility, vendor business continuation planning /execution or the behavior of contract resources under duress. But there are steps they can take closer to home to lower risk. This starts by ensuring that strong project management, process orientation, onsite knowledge retention and good system documentation are used in offshore projects. These actions will make it much easier to transfer work back onsite if necessary. Other best practices include careful evaluation/selection of offshore projects and appropriate utilization of heavily offshore leveraged projects.

For every potential or existing offshore project, the project manager should develop a resource backup plan should the unthinkable happen. The plan should include actions closer to the project manager's control, rather than actions in the control of vendor, government or offshore resource. If the cost of this plan is not reasonable, the project may not be an appropriate candidate for offshore development.

Clients can also lower their risk by adopting a technique from investment portfolio management - diversity among asset types. Offshore work should be spread across multiple facilities in different countries/geographical areas to hedge political risks. Offshore options outside of the India/Pakistan region continue to widen, including the Philippines, Mexico, China, Russia and former Soviet bloc countries. None of these regions offer the abundance of technical resources of India but they do have the benefit of lowering political risk in your offshore project portfolio.