



*"The Perfect Fit for
Your Business"™*

ROBERT H. CARPENTER, JR.

ATTORNEY AT LAW
5912 CASTLEBAR LANE
PLANO, TEXAS 75093

—
TELEPHONE 972.473.4834

—
email: Bob.Carpenter@CarpenterLaw.net

—
www.CarpenterLaw.net

November 2004

Offshore Outsourcing — An Inevitability

Offshore outsourcing, or what is sometimes called “offshoring,” is inevitable; it is a basic business necessity. As Americans become less enchanted with certain work, such as repetitive keying and coding, and demand higher pay (and require greater general and administrative expense support) for almost any work that they perform, competitive pressures will drive selected business processes offshore where costs are less.

Almost half of information technology organizations have outsourced some work offshore. The best candidates for the ever-increasing offshore “pie” are business processes that are widely known and easily measured – like bank “back office” functions.

in·ev·i·ta·ble (ĭn-ĕv-ĭ-tə-bəl) *adj.*

1. Impossible to avoid or prevent.
2. Certain to happen.

Offshoring information technology services can be tricky; and consumers must be highly aware. In the heavily regulated financial services industry there are plenty of “second-guessers” (and not without good reason) who will evaluate every offshore move.

Earlier this year (in June 2004) the FDIC released a staff study titled *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks*.¹ In this “white paper” the FDIC weighed in with its view of offshoring risks. Not surprisingly, in reading *Offshore Outsourcing* one gets the distinct impression that the FDIC, and probably the other Federal and state bank regulatory agencies, will be giving a very close look to offshoring risk management practices.

Many community-based financial institutions will find themselves in the midst of what is, at least this year, partially a political debate on offshoring and what is most certainly a trend to reduce costs, augment capacity and improve efficiency and time to market. How? Why?

¹ Fed. Deposit Ins. Corp., OFFSHORE OUTSOURCING OF DATA SERVICES BY INSURED INSTITUTIONS AND ASSOCIATED CONSUMER PRIVACY RISKS (2004) www.fdic.gov/regulations/examinations/offshore/offshore_outsourcing [hereafter OFFSHORE OUTSOURCING].

Because most have decided to outsource routine data processing functions to vendors – not a bad choice when a business is intent on focusing on its core competencies and leaving the more routine or ancillary business processes to experts – that in an ever consolidating marketplace are looking more and more to offshoring as an enterprise-wide competitive strategy. That choice places those community-based financial institutions in the FDIC’s highest risk category for offshore outsourcing.

Business Models

The FDIC categorizes a financial institution that has outsourced its data processing to a vendor that employs offshore resources to accomplish its services as the “indirect third party” model. While both customer and vendor are domestic operations, the vendor subcontracts some of its responsibilities to an overseas business.² The charge here, according to *Offshore Outsourcing*, is “controls may not exist to preserve the integrity of customer and bank data.”

Actually, the risk is much broader than that. The viability of the subcontractor, the reliability of its employees and the security of its workplace are among the many factors that must be evaluated and ensured.

There are, within the indirect third party model, three subcategories that the FDIC does not explicitly identify and that have differing risk profiles. First, the vendor that offshores work could have a foreign captive. This would seem, according to *Offshore Outsourcing’s* analytics, to present the least risk to the customer. Second, a vendor could joint venture an offshore operation that would provide some direct measure of control. And, finally, the vendor could subcontract its work to an offshore provider with whom it has a legal agreement for services.

Without arguing the theory or basis for the FDIC’s views, a community-based financial institution that has outsourced a critical, but non-core function to a third party, needs to know what to do to prepare for expected regulator and auditor scrutiny of its data processing vendor arrangements.

Risk Analysis

The FDIC correctly notes that offshoring has inherent risks that are in many ways similar to those in domestic outsourcing. However, in the five traditional risk categories – Reputation Risk, Operations/Transactional Risk, Compliance Risk, Strategic Risk and Credit Risk – offshoring adds new, and often troublesome, dimensions that relate to the additional Country Risk generated by foreign operations. And, then, there’s Country Risk itself.

Unfamiliarity with Country Risk, or Political Risk as it is sometimes called, has driven some financial institutions to attempt to eliminate it entirely by prohibiting any subcontracting for their data processing work to foreign locations or by obtaining a penalty-free termination right for the customer if the vendor elects to offshore any of the customer’s work. Frankly, neither option offers the financial institution any advantage. Offshoring is an inevitable outcome for any competitive business operation. Learning to identify and deal with the potential impacts of new offshoring risks is the challenge.

² The FDIC staff identifies three other offshoring business models. In order of decreasing risk, they are: “Direct third party” in which a financial institution customer subcontracts its work directly with an overseas provider and for which controls exist only through contractual terms. “Joint venture,” a partnership between a domestic customer and a foreign entity where control is shared. And, a “captive direct” arrangement where the domestic financial institution relocates its own operations offshore and where dedicated management and substantial at-risk investment incents best control and least risk.

Country Risk, and the unique dimensions that offshoring adds to the other five more traditional risks, may be controlled by focusing on choice and performance, two things that should be addressed in any outsourcing agreement. Rights and remedies (*i.e.*, choices) and performance criteria, to which a customer holds its primary vendor accountable, can serve to optimize risk in the many risk dimensions of offshoring.

Risk-Optimizing Actions

Decision makers, and their advisors, are in the business of optimizing risks rather than eliminating them. They expect the greatest reward for an acceptable, commensurate risk. In approaching the decision to outsource, vendor management is key. Nothing will replace due diligence in selecting and monitoring a data processing vendor, but how can one control offshoring risks that one cannot easily “see”?

As the FDIC implies in *Offshore Outsourcing*, contractual arrangements may be the least effective in controlling risks in an outsourced business process. Poorly conceived contractual provisions make that problem even worse. For instance, in the case of poor performance, a termination right might not even be the most effective remedy or the path that a customer wants to take. What should a financial institution customer really want from its data processing vendor? How does that relate to that vendor’s decision to offshore work?

Subcontracting

Almost any vendor of any product or service must subcontract some work. The very nature of the subcontractor relationship implies that the prime contractor remains responsible for the work that is sent out. If subcontracting is so much a part of business (and it is) and offshoring is inevitable (and it is), then the customer needs to know what work is being subcontracted and to whom and what controls the prime contractor has put in place to protect the customer’s work.³

The responsibility must be on the vendor to inform the customer, in advance and in a timely manner, of the offshoring decision so that the customer can fully and accurately evaluate the effects of that decision upon its business. Has the vendor established adequate data security measures and oversight? Does the vendor have a business resumption plan if the offshore operation shuts down? These, among others, are important considerations for the customer.

Customer and vendor should establish some measure of “partnership” in this evaluation process. Offshoring must be a good business decision, for both; an unhappy customer benefits no one. The vendor must be held accountable for a solid business decision and required to demonstrate that to the customer, and its auditors and examiners alike, in the details of its offshoring plans.

Performance Standards

A material breach of a contract (*i.e.*, one that is in substance, rather than form, important to the non-breaching party) generally allows the non-breaching party to terminate. But that may be an ineffective remedy in the case of a long-term, heavily invested data processing relationship. In fact, the customer almost never wants to terminate, but rather wants a means to incent its vendor to perform.

³ If a customer considers specific business processes too sensitive or so integral to its successful operation that offshoring would present an unacceptable risk, the customer should identify these business processes in the data processing contract and obtain the vendor’s agreement that they may not be offshored without the consent of the customer.

That's why performance criteria, also known as "service level agreements" or "SLAs," are so important. And, they must apply not only to domestic-supplied, but also foreign-supplied services. Timely vendor reporting obligations and appropriate remedies for important failures must support them.

SLAs must be objective and quantifiable, and timely reporting and performance against them must be within the vendor's capability. In negotiating SLAs, a customer should evaluate the vendor's past performance against the same or similar criteria, either for a representative customer or some portion of the vendor's customer base. Most importantly, the customer should insist on SLAs that are meaningful to its own customer-service objectives. The customer must boil SLAs down into what a failure of performance will mean to its end-user customers.

What should happen if the vendor fails a performance standard? There may be some single SLA for which a failure should be *per se* a material breach that gives the customer an immediate right to terminate; but this would be the exception. More often the repetitive failure to meet a particular SLA, which will focus on a very specific service objective, should trigger a remedy.

Thus, not only the criteria, but also the frequency of failure should be considered in developing SLAs. Then, based upon the severity of the resulting failure or failures, a remedy is created. Most often, the customer will want to incent the vendor to better performance by some monetary payment or credit. But such payments should not be the sole remedy because they will not normally cover the damages (both monetary and reputation) that repeated failures could cause.

After some number of repeated failures of either a single criterion or of multiple criteria relating to various performance functions, the customer should have the option to terminate its outsourcing arrangement and find a new vendor. Importantly, in no event should there be any distinction between a failure caused by the vendor and one caused by the vendor's subcontractor, especially an offshore one.

Wise Choices

The community-based financial institution that carefully chooses a vendor based upon a thorough due diligence, closely monitors the vendor's use of offshore capabilities (including less risky and more direct foreign arrangements) and holds the vendor strictly accountable for its acts and those of its subcontractors can reduce risk in "indirect third party" offshoring. Wise choices will allow that financial institution to enjoy the benefits of a highly competitive data processing vendor with appropriately limited risks.

© 2004, 2007 Robert H. Carpenter, Jr.

This client newsletter is for informational purposes only, and is not intended to be legal advice. Transmission of this newsletter is not intended to create, and its receipt does not establish, an attorney-client relationship. Legal advice of any nature should be sought from legal counsel.

IRS CIRCULAR 230 DISCLOSURE: Notice regarding federal tax matters: Internal Revenue Service Circular 230 requires us to state herein that any federal tax advice set forth in this communication (1) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed by federal tax laws, and (2) cannot be used in promoting, marketing, or recommending to another person any transaction or matter addressed herein.