

OUTSOURCING IN TOUGH ECONOMIC TIMES

James E. Meadows
FSB Legal Counsel,
a Fisher Broyles LLP
Atlanta, Georgia
(404) 806-7149
meadows@fsblegal.com

TOP CUSTOMER QUESTIONS

1. What protection can you build in against the supplier going under (and what steps can/should you take once that appears to be on the horizon)?
2. What is typical regarding termination rights tied to service level performance, and how should a customer approach negotiating an appropriate termination for convenience “penalty”?
3. What is the best way to approach negotiating the allocation of risk and liability issues (e.g., allocation of responsibility, limitations of liability and exclusions, indemnification), and are vendors willing to accept more or less liability in certain types of deals (eg., collocation agreements versus traditional IT infrastructure arrangements) and/or with respect to certain types of exposures (e.g., data breach)?
4. Should I consider renegotiating my existing outsourcing relationships? If so, how, and in what areas should I be looking for improvement?
5. Is now a good time to take work offshore?
6. Is insourcing a viable “out” sourcing alternative, and what is involved in making that assessment?
7. Do you have any strategies that are likely to be particularly effecting in the current market?
8. How do you determine at the outset what kind of document is appropriate for an outsourcing transaction, when the range seems to vary from pretty high level (20-30 pages) to very detailed and requirements-heavy (hundreds of pages/multiple exhibits)?
9. How can you structure outside counsel support for these transactions and manage the budget for the negotiation of these deals?

Here we are on November 5, 2009, and it seems that the world wasn't coming to an end after all. So, how does this affect the world of outsourcing? I would assert that now is the time to start looking at your existing outsourcing and offshoring relationships, and your strategy moving forward, because companies that have spent time preparing for the eventual uptick could be creating a competitive advantage moving forward. Let's take a look at some questions and comments provided by a number of my past and present outsourcing customer clients:

1. What protection can you build in against the supplier going under (and what steps can/should you take once that appears to be on the horizon)?

Planning for the scenario where an outsourcing supplier's performance may be negatively impacted by its financial condition is really no different from protecting against any other situation which may affect the supplier's performance. The key is anticipating the possibility and then planning for the contingency, and it is never too late to engage in such effort (whether the contract has already been executed or the negotiations are just beginning. See the article attached as Appendix A – "Business Continuity ... Yours and Theirs: Contingency Planning from the Outset to Minimize Potential Future Impact."

2. What is typical regarding termination rights tied to service level performance, and how should a customer approach negotiating an appropriate termination for convenience "penalty"?

a. Service Level Performance. Before even thinking about termination as a remedy, the first step involves defining the performance measurements up front, which is usually comprised of the following steps: (i) establish performance objectives; (ii) define the metrics (and associated standards); (iii) prepare the Service Level Agreement; (iv) determine how you will ascertain/prove compliance (e.g., reports, third party monitoring), and only as the last step (v) craft the remedies for non-compliance.

b. Termination (Exit Plan).

i. Types of Termination. TIP: Each potential basis for termination should be carefully considered in detail, including the effect of each type of termination.

1. Breach (analyze by party in breach and by type of breach)
2. Convenience (i.e., buy-out)
3. Languishment (i.e. failure of relationship to achieve expectations)

4. Other strategic events (i.e., for “good reason”—as opposed to “cause”—including mediocrity)
5. Bankruptcy events
6. Change in control

ii. Effect of Termination

1. Wind-down period
2. Transition to alternative offering (including transition assistance)
3. Post-termination obligations, including title or ongoing rights to various deliverables and intellectual property, and customer relations and customer data issues

c. Termination Charges Methodology. **IF** the Customer is required to pay a Termination Charge, it should be calculated for the portion of the Services that are to be terminated (the “Terminated Services”), which may require more detail around the specific elements that might be terminated and/or applying a percentage to one or more of the Termination Charge elements (e.g., a portion of the applicable Termination Charge amount, proportional to the value of the Resource Units that are included in the Terminated Services). One way of looking at Termination Charges is to consider whether and to what extent, based upon the reason for termination (e.g., pure convenience, change of control), the Supplier should be permitted to recover within each of the following categories:

- i. Unrecovered Investments, which facilitates recovery of certain of the Supplier’s start-up costs related to entering into the relationship in the first place. This element would typically disappear over time and as the reason for the termination moves away from being characterized as being for convenience.
- ii. Financed Costs, which addresses any costs financed as part of the Charges (e.g., backloading of periodic monthly Charges). This element is typically included in the Termination Charges, even if not purely for convenience.
- iii. Shut Down Costs, which address the Supplier’s recovery of certain shut-down or make-whole costs.
- iv. Termination for Convenience Charge, sometimes expressed as a percentage of the monthly Base Charges for the terminated

Services multiplied by the number of full months remaining in the Term.

d. Invoicing. Note that the parties may agree to the payment of certain elements of the Termination Charges at different times. For example, Supplier might invoice Customer for the Unrecovered Investments Termination Charge and Financed Costs Termination Charge within a prescribed time period following the Termination Notice Date, and then invoice Customer for the Termination for Convenience Charge within a prescribed time period following the Termination Effective Date.

e. Shut Down Costs should consist solely of the reasonable costs that Supplier actually incurs as a result of the early termination of the Agreement or Statement of Work with respect to the Terminated Services. Within a prescribed time period following the Termination Notice Date, the Supplier should be obligated to provide the Customer with an itemized calculation of Supplier's good-faith estimate of the Shut Down Costs for the Terminated Services as of the Termination Date. The Supplier should provide any applicable documentation that is reasonably necessary for the Customer to validate such calculation, and the Customer should also be entitled to audit Supplier's estimated Shut Down Costs and supporting documentation in accordance with the underlying Agreement. The Supplier should only be permitted to invoice the Customer for amounts payable as Shut Down Costs as they are incurred by the Supplier.

f. Supplier Mitigation. The Supplier should use commercially reasonable efforts to avoid incurring any termination costs and to minimize the costs incurred including, for a reasonable period of time following the Termination Notice Date, seeking to recover amounts previously paid to a Third Party. The commercially reasonable efforts to be employed by Supplier should include, to the extent applicable:

- i. providing Customer with (i) a list of all Supplier-owned Equipment, Supplier Licensed Software and any applicable leases, licenses and other Third Party contracts used exclusively to provide the Terminated Services, and (ii) the costs associated with each;
- ii. working with Customer to identify commercially reasonable means to avoid or minimize such costs;
- iii. offering to make such Equipment, Software and any such leases, licenses and other Third Party contracts available to Customer (or a Successor Supplier);
- iv. attempting to redeploy the remainder of any such Equipment, Software and Third Party contracts within Supplier's organization if, and as soon as, commercially reasonable;
- v. negotiating with any applicable Third Party to eliminate or reduce the fees or charges to be incurred; and
- vi. subject to any limitations contained in the applicable licenses or other Third Party contracts, selling, canceling or otherwise disposing of any such Equipment and Software and any such

leases, licenses and other Third Party contracts that cannot be redeployed.

The costs to be reimbursed by Customer should cease to accrue following the redeployment or use of such Equipment, Software and Third Party contracts for any other purpose and should be reduced by the net proceeds received from any sale or other disposition.

Shut Down Costs should not include any amounts paid to the Supplier with respect to Equipment and Software to the extent Customer or the Successor Supplier elects to purchase such Supplier-owned Equipment or Software.

g. Equipment. The Shut Down Costs could include the following for Equipment that the Supplier uses exclusively for the provision of the Terminated Services and that Supplier is unable to redeploy or otherwise avoid pursuant to paragraph (f) above:

- i. Leased Equipment. With respect to Equipment that is leased by Supplier, the Shut Down Costs could consist of: (a) any termination or cancellation charges (or similar amounts) that Supplier is contractually required to pay to a third party in connection with the early termination of such lease; and (b) any non-cancelable charges that Supplier is contractually required to pay to a third party during the remaining term of such lease. The Customer should have visibility into these costs prior to the commitments being made during the term of the Agreement.
- ii. Supplier Owned Equipment. With respect to Equipment that is owned by Supplier, the Shut Down Costs could consist of the net book value of such Equipment as of the Termination Date (calculated using a straight-line method over a period equal to the applicable asset useful life).

h. Software and Other Third Party Contracts. The Shut Down Costs could include the following for any Supplier Licensed Software or other Third Party contract (other than any Equipment lease) that Supplier uses exclusively for the provision of the Terminated Services, and requires Supplier to pay termination or cancellation charges: (a) any termination or cancellation charges (or similar amounts) that Supplier is contractually required to pay to a Third Party in connection with the early termination of such lease, license or other contract; and (b) any non-cancelable charges that Supplier is contractually required to pay to a third party during the remaining term of such lease, license or other contract. As with Equipment lease costs, Customer should be given visibility into these costs prior to the commitments being made during the term of the Agreement.

i. Supplier Employees. Always a very sensitive topic! With respect to Supplier's employees who are primarily assigned to the provision of the Terminated Services as of the Termination Date ("Eligible Supplier Employees"), the Shut Down Costs could consist of the following severance or redeployment costs reasonably incurred by Supplier:

- i. Redeployment. The actual wages paid to or on behalf of Eligible Supplier Employees who are not severed by Supplier and are awaiting redeployment provided that (i) such reimbursement shall terminate upon the redeployment of such employee for any other purpose and (ii) the total period of such reimbursement shall not extend for more than a reasonable period of time (e.g., thirty (60) days) after such employee ceases to perform Services; or
- ii. Severance. Only in the early stages of the relationship (i.e., because the Customer should not be responsible for long-time Supplier employees and commitments specifically targeted at the work for Customer should not necessarily be for the duration of the Agreement), the actual severance payments made to Eligible Supplier Employees pursuant to the then-current Supplier severance policy, *provided* that (i) notice of severance occurs within a short period after each such employee ceases to perform Terminated Services, and (ii) the severance payments made to such employees do not exceed those available to similarly situated employees under the Supplier severance policy in place as of the Termination Notice Date.

3. What is the best way to approach negotiating the allocation of risk and liability issues (e.g., allocation of responsibility, limitations of liability and exclusions, indemnification), and are vendors willing to accept more or less liability in certain types of deals (eg., collocation agreements versus traditional IT infrastructure arrangements) and/or with respect to certain types of exposures (e.g., data breach)?

- a. Representations, Warranties and Covenants
 - i. Security Breach - Responsibility, costs (mailings, call centers, etc.), class action liability and other issues are getting contentious.
- b. Limitations of Liability
 - i. Dollar Caps. TIP: Consider, at a minimum, direct damages likely to be sustained. For example, in security breach hypothetical, consider all likely costs, including direct liability to third parties, mailings, call centers, etc.

ii. Exclusions from Cap

- Confidentiality and proprietary rights
- Indemnification from third party claims and government fines and penalties
- Gross negligence and willful misconduct

iii. TIP: Consider from each party's perspective.

c. Exclusions of Certain Types of Damages

i. Types

- Consequential, special, incidental, indirect, etc. damages
- Lost profits
- Loss of use or data

ii. Exclusions from Exclusion

1. Confidentiality and proprietary rights
2. Indemnification from third party claims and government fines and penalties
3. Gross negligence and willful misconduct

d. Indemnification

- i. Intellectual Property Infringement
- ii. Breach of Warranties
- iii. Privacy Violations
- iv. Compliance with Laws
- v. Gross Negligence and Willful Misconduct
- vi. Customer Claims. TIP: Focus on the party with the direct relationship with the customer that is of most relevance to the disputed claim. That party may be in the best position to protect itself from such claims (e.g., by contract).

e. Other Remedies

- i. Liquidated Damages
- ii. Termination (discussed above)

f. General Approach

- i. Consider the events likely to cause a covered problem.
- ii. Look at responsibility objectively.
- iii. Evaluate responsibility by type and nature of services.
- iv. Determine extent of responsibility.
- v. Consider the extent of damage likely to be sustained.
- vi. Evaluate the type(s) of damage likely.
- vii. Quantify the damages by type.
- viii. Match responsibility with damage.
- ix. Determine ability to effectively mitigate.
- x. Assess available leverage.

g. Hypothetical 1: Allocation of liability in collocation agreements versus managed server arrangements ... where the vendor, in a collocation agreement, says “we are like a landlord” and therefore they are not willing to assume any liability.

h. Hypothetical 2: Security Breach - Responsibility, costs (mailings, call centers, etc.), class action liability and other issues are getting contentious.

- i. Some suppliers are becoming more restrictive in accepting risk, especially in the data security and credit card compliance areas, and are seeking lower liability limits for data loss. The risks of experiencing a data security incident include not only financial costs (the costs of notifying individuals alone can be high), but also significant embarrassment and reputational damage to the culprit company.
- ii. On the other hand, buyers are becoming more sophisticated as well, devoting significantly more energy to incorporating new risk and liability provisions with respect to data loss and the consequences of breaching security data obligations.

4. Should I consider renegotiating my existing outsourcing relationships? If so, how, and in what areas should I be looking for improvement?

a. Time to capitalize on the current market opportunity – Strong buyers’ market for outsourcing services? If so, for how much longer? Time to take a long, hard look at your contracts, relationships, and strategies. Two questions:

- i. What should I be doing now to improve performance?
- ii. How can I best position the organization for the future?

b. Renegotiation must create value for both parties, but don't assume anything and don't think only in terms of your own perspective – “walk a mile in your supplier's shoes” – you might be surprised by the elements of value that you find (that may not cost you anything)!

c. But my current agreement doesn't expire for another ___ years ...!

- i. Early renewal or extension of the term of an existing agreement (more likely to be an available approach, given overall shorter deal terms over the past decade).
- ii. Save the Supplier a lot of money in business development and deal pursuit costs.
- iii. Positive publicity? Announce the deal to showcase your extension or renewal to new and existing customers, their investors, and their bankers.

d. Negotiable concessions:

- i. Price cuts (or more efficiency)
- ii. Additional services (or reductions in scope)
- iii. More favorable contractual terms and conditions
- iv. Upgrades to infrastructure
- v. Better committed service levels

e. Be creative: One consultant has proposed the radical idea of the customer volunteering to accelerate its payment terms (i.e., in response to tight credit markets) in exchange for concessions. Credit markets are still pretty tight for you and for the service provider community.

- i. Time value of money associated with the faster payments
- ii. Detailed cost/benefit analysis to ensure you correctly assess your additional financial costs, the estimated financial benefit for your supplier, and the value of negotiated benefits for all parties -- both financial and non-financial.

f. Strategic Planning

- i. “Circle the Wagons” – Consider enhancing your business relationships with your best supplier(s).
- ii. Revisit joint ventures (e.g., where a supplier and a business partner that traditionally would have been a customer jointly develop a service offering that benefits the partner as a “customer” and enables the joint venture to quickly productize a service offering for the broader market).

5. Is now a good time to take work offshore?

a. Timing: Many offshore suppliers have experienced flat revenue during 2009, and may be willing to accept smaller profit margins in exchange for more business.

b. Benefits to creation of a long-term, enterprise level offshore strategic plan include enhancing:

- i. Long-term sustainability
- ii. Leverage for negotiations and performance levels
- iii. Better cohesion across business units
- iv. Lower infrastructure and management costs
- v. Effective overall cost management.

c. Diligence and Site Visits: Be sure to document clear objectives for the site visits and objective evaluation criteria to assess operations, capabilities, and fit.

6. Is insourcing a viable “out”sourcing alternative, and what is involved in making that assessment?

a. What is it? Repatriation of existing outsourced functions. The primary business benefit is often cost reduction while maintaining full control of the functions in scope. KEY is to treat the process the same as “outsourcing internally.”

b. Are you ready to insource? Need to conduct a detailed insourcing assessment to define the baseline for expected benefits, just as you would for ANY sourcing strategy.

- i. Operational – Will you be able to improve the processes within the delivery model, and enhance project delivery ability?
- ii. Organizational – Will you be able to optimize resources?
 - 1. Access to current and future skills needs
 - 2. Ability to offer viable career paths
 - 3. Ability to attract/retain in demand skills
 - 4. Platform scalability
- iii. Service – Will you be able to ensure service consistency?
 - 1. Response to user needs
 - 2. Service levels and other performance measurements – minimize complacency
- iv. Strategic
- v. Financial – Ability to support business case

c. Application of structured methodology to develop a strategy and implementation plan.

- i. Business case
 1. Data collection
 2. Analysis
 3. Decision point
- ii. Solution design
 1. Create resource plan
 2. Transfer and/or acquire rights to required contracts
 3. Develop technology plan
 4. Decision point
- iii. Implementation and transition

7. Do you have any strategies that are likely to be particularly effecting in the current market?

a. Multisourcing involves (i) selecting a host of best-of-breed suppliers; (ii) negotiating “comparable” deals with each; and (iii) allowing these “pre-qualified” suppliers to bid on projects/engagements as they arise.

8. How do you determine at the outset what kind of document is appropriate for an outsourcing transaction, when the range seems to vary from pretty high level (20-30 pages) to very detailed and requirements-heavy (hundreds of pages/multiple exhibits)?

- a. See Appendix B - Representative Master Services Agreement Table of Contents

9. How can you structure outside counsel support for these transactions and manage the budget for the negotiation of these deals?

a. Create negotiation efficiencies: KEYS to negotiating a deal in a compressed time frame

- i. TIP: Understand what negotiating a deal within a shorter window REALLY means
 - Anticipating the end product of the negotiations
 - Conscious decision NOT to address (or NOT to address ADEQUATELY) certain issues

- ii. Establish (or know) your negotiating bottom line (i.e., understanding what benefits that you “can” receive from the relationship/other party, and what it is willing to give in return)
 - Distinguish between “needs” and “wants”
 - Cover as many potential issues as possible
 - Negotiating team comfort with positions
- iii. Know (or estimate) the other party’s bottom line
 - Understand “why” other party wants the deal
- iv. Establish (in advance) strategy for achieving “wants”
- v. Negotiation Procedures
 - Identification of the participating representatives from involved or affected units
 - Pre-negotiation alignment meeting
 - Development of negotiation plan
 - Negotiations
- vi. Obtain “early” senior manager buy-in (both legal and non-legal)
 - TIP: Time spent reviewing the initial draft of the agreement and relevant schedules/exhibits (and discussing the issues therein) will save time in reaching final agreement, and allow negotiating team to put other party on defensive (as opposed to other way around). In other words, complete the “internal” negotiations before commencing “external” negotiations.
 - Empowering the negotiating team to speak for the company
 - Authority level constraints of negotiating team
 - Immediate (e.g., 24 hour) access to the business person(s) responsible for specific subject matter (e.g., compliance, security, intellectual property, etc.)
- vii. Identify viable solutions early, and use that information tactically

- Plan on negotiating session breaks to discuss strategy (not necessarily when key issue is at an impasse, but hopefully before key issue comes up)
- Don't perform line-by-line "walk" through draft agreement too early
- Use lawyer-to-lawyer discussions to identify "pressure points" early, and use the information gathered to structure negotiations

viii. Term Sheets

- Important to defining basic deal (see above)
- Move quickly to initial draft of agreement by not spending too much time defining "everything" the parties agree upon (while ignoring the parties' differences).
- Avoid "letters of intent," "memoranda of understanding," etc. – they almost NEVER benefit the customer
- Notwithstanding the foregoing, if a letter of intent must be prepared (for business, strategic or other reasons), it should generally be non-binding (with the sole exception as provided below).
- If services are to be performed prior to execution of a definitive agreement, the letter of intent should also contain certain minimum terms for the protection of the customer. Those terms will include (i) a clear cap on the amounts to be paid by customer under the LOI, (ii) customer ownership of deliverables created, (iii) protection of customer intellectual property (including confidentiality), and (iv) no publicity without customer consent and approval of subject matter.

Appendix A

Business Continuity ... Yours and Theirs: **Contingency Planning from the Outset to Minimize Potential Future Impact**

By James E. Meadows, Partner
FSB Legal Counsel
meadows@fsblegal.com

Companies typically consider offshore outsourcing as a means to create flexibilities and opportunities that they may not otherwise be able to realize domestically. To realize such benefits, however, the customer must be prepared to overcome a series of additional (or modified) legal issues that are associated with such transactions and their resulting relationships. One such issue is business continuity. Business continuity is the ability of a company to continue business operations notwithstanding changes to the company or its trading partners, and whether such changes are caused by unforeseen circumstances or otherwise.

A wide range of circumstances can impact business continuity. These circumstances can generally be classified into one of two general categories: those occurring to the company directly, and those occurring as a result of the company's relationships, contractual or otherwise, with third parties. While the company can create its own business continuity concerns, whether through unwise business decisions, accounting improprieties or otherwise, contingency planning to address direct circumstances generally seeks to anticipate possible, albeit unlikely, causes (e.g., force majeure events). This article focuses on contingency planning for circumstances involving third party relationships (specifically, offshore or near-shore outsourcing) that could adversely impact business continuity.

The customer to an offshore outsourcing transaction will have a vested interest in ensuring that its business will continue uninterrupted in the event that one or more of its offshore vendors encounters circumstances that could prevent it from performing. Those circumstances could include the unexpected (similar to those that might affect the company/customer itself) and the situations involving the failure of the vendor to perform, or to perform adequately. Customers should plan for both sets of circumstances by ensuring that its vendors are focused on the unexpected, and by building contractual protections (and backup plans) to address performance failures.

This article provides a roadmap for addressing vendor situations that could impact customer business continuity, and walks potential offshore customers through the benefits of combining a contractual exit strategy (as long as the customer has an adequate backup plan) with proactive relationship building, focusing on (i) joint contingency planning, attempting to address as many contingencies as possible, (ii) conducting diligence on the vendor's disaster recovery plan and managing the plan throughout the

relationship, and (iii) implementing strong governance mechanisms and an effective communication plan. By targeting these relationship elements, the customer can develop a plan to keep the vendor as focused on business continuity as the customer itself.

Exit Strategies

Exit strategies generally define what happens (or is intended to happen) either upon the natural expiration of an offshore relationship, or in the event of an early termination of that relationship. Contractual exit strategies are difficult to negotiate, and even more difficult to implement. They are difficult to negotiate because neither party is entering into an offshore outsourcing transaction for the purpose of terminating the relationship, certainly not the vendor. In general, it will be incumbent upon the customer to affirmatively raise the issue, because vendors universally prefer long-term contracts to provide for more time to recover startup costs and maximize the total contract value, and because the longer a vendor's services are used, the more dependent a customer becomes on the vendor. Contrast this with the customer's desire for shorter terms to maintain flexibility and options.

Exit strategies work by establishing that certain events will trigger the customer's right to terminate the relationship, or a specific aspect of the relationship, either immediately or over a prescribed period of time (e.g., following a wind-down or transition period). Triggering events often include: (a) varying types of breach by the vendor; (b) bankruptcy or insolvency events (although bankruptcy as a trigger event will generally not be enforceable, or at least not in the United States); and (c) force majeure events, with certain events triggering immediate exit, and other events triggering termination based upon length of time incurred. The exit strategy will then address each party's rights and obligations associated with the termination (before, during and after), including:

- The vendor's obligation to transfer any customer data or information obtained or stored by the vendor to the customer or its designee (in a specified format). From the customer's perspective, this right should be unconditional and unrestricted, and not conditioned upon the payment of any fees due or alleged to be due. Note that such data/information transfers (whether to the customer or to a separate jurisdiction) should be occurring regularly in an offshore relationship.
- A means to establish the fees for any transition assistance provided by the vendor. Otherwise, the customer will have no leverage and may be forced to pay unusually high fees (e.g., published time and materials rates) for the transition assistance. The customer will also want to protect against being charged incrementally for base line resources redirected to transition support (i.e., double billing). Finally, the transition assistance fees should contemplate the basis for termination (e.g., no profit factor for transition assistance required where the customer is terminating for cause).
- A minimum period of time in which the vendor will continue to provide the services at contract rates as the services are migrated back to the customer or to

another vendor. During this same time period, provision should be made for knowledge transfer *back* to the customer (or its designee), to the extent such knowledge transfer has not been happening throughout the term of the contract (... which it should).

- If any vendor employees are necessary for the services, the customer's right to interview and hire these employees, although any such personnel decisions will necessarily implicate visa/INS compliance considerations.
- If any equipment, software or other technology is essential to the services, the customer's right to acquire these assets (and terms associated with such purchase), although purchasing physical assets in offshore jurisdictions will present its own set of unique considerations (tax, doing business in a foreign jurisdiction, corporate structure and otherwise).

In formulating the exit strategy, the customer should also consider: (i) requiring the vendor's cooperation in the migration of the services to another service provider (perhaps even a competitor); (ii) the intricacies of unwinding the services associated with the particular infrastructure deployed by the vendor (i.e., obviously is easier to transition from a dedicated service than from one that is shared among multiple vendor clients); (iii) unwinding the vendor's applicable subcontractor relationships (which the customer should identify during the diligence phase of the procurement process, noting potential termination impacts); and (iv) export/import regulations that may impact transition of operations/services back to the United States or to an alternative service provider.

The concept of an "exit strategy" sounds great and certainly a logical topic for discussion in the negotiation of an offshore outsourcing transaction. Be aware, however, that they often fail in an offshore context if adequate consideration is not given to what actually needs to happen upon termination. An exit strategy will only succeed if a robust "backup" plan is in effect, and that backup plan is a part of the customer's broader business continuity plan. For example, if the customer is operating its sole call center for a given process in India and the exit strategy is implicated, the customer should ask itself whether it expects to be able (in a relatively short timeframe) to complete all of the steps necessary to transition the call center away from the vendor. Does the customer have the requisite operational knowledge (not always a given, if knowledge transfer has not been occurring continuously during the relationship)? Does the transition include/require the vendor's employees? So, the ultimate question may be whether, or the extent to which, termination is a viable contingency plan.

Contingency Planning

Exit strategies in connection with individual offshore agreements only work when they are part of the customer's global business continuity plan. In this case, we are talking about the customer's business continuity plan for the specific function or process. This plan will be implemented (in whole or in part) by the vendor, because the contingency plan may include shifting the function or process to another location, perhaps in a different country, and perhaps operated by a different vendor (i.e., multi-

sourcing). As discussed above, contingency planning should cover both foreseeable and unforeseeable events.

Developing, implementing and managing a contingency plan around a given process or function is not simple. Successful contingency plans (always viewed in hindsight after they are triggered) will have contemplated all credible worst case scenarios. They will include a plan, not only for operations during the triggering event, but also for restoration of services to historic or desired levels as soon thereafter as possible. They will address such administrative matters as identifying the team(s) (both internally within the customer organization and externally through representatives of the applicable service providers and business partners) for handling contingencies, and providing for periodic testing of the contingency plan.

In addition to addressing what happens “when” a triggering event occurs, contingency plans should also address what needs to be happening “before” the triggering event occurs; for example, during the term of an offshore relationship (e.g., ongoing knowledge transfer). Central to the issues addressed in this part of the contingency plan will be intellectual property rights, and ensuring that the customer will have the ability and the necessary legal rights (whether through ownership, license or otherwise) to recover operation of the function or process, or transition same to another provider. The plan will generally also provide for the customer’s right and ability to retrieve assets in the event of a service provider’s insolvency or nonperformance, even if claims or liens (permitted in certain jurisdictions) have been (or can be) filed by employees of the service provider and/or various subcontractors against the service provider, against the customer directly, or against any of the assets to be recovered. In short, the process for developing the plan will determine the substance of the contingency plan, and thus the ultimate effectiveness of the plan.

When the customer’s contingency planning includes multi-sourcing, the exit strategy for a particular offshore relationship may be made easier by consideration in the broader scope. Obviously, if two vendors are providing the same services to the customer (assuming that it is practical to do so), one vendor may be able to serve as the backup for the other, and vice versa, if each has the ability to scale up to cover the work performed by the other. This is one of the advantages of a multi-sourcing business strategy. Other advantages include (a) the ability to scale to address future business needs, (b) healthy competition (e.g., negotiating change orders), and (c) assembling or developing, and then deploying, best practices (based upon what each vendor does best). Often, however, a multi-sourcing approach either will not work (e.g., because it may not be feasible to divide a business or technology function among two or more vendors) or may not be desirable from a business perspective. The traditional business reasons given for sole sourcing include (1) establishing a trusted relationship, (2) volume benefits (e.g., cost, scale), and (3) lower management costs.

Even if the customer cannot implement a true multi-sourcing approach, to the extent economically feasible, the customer should establish and maintain backup vendor

relationships for critical functions outsourced. In developing an offshore strategy, the customer should consider providers with geographically disparate facilities. At a minimum, the contract needs to provide the contractual flexibility to establish such backup relationships, both from an affirmative (e.g., cooperation from the principal vendor) and negative (e.g., unrestricted right to engage third parties—i.e., non-exclusivity) perspective. Of course, the vendor will generally argue that providing such flexibility could ultimately enable the customer to cherry-pick services during the term of the agreement, thus fundamentally altering the basic deal.

Disaster Recovery Plans

How can a customer ensure that its offshore vendor(s) is just as focused on business continuity as the customer? Answer: (i) ask to see the vendor's disaster recovery plan; (ii) conduct extensive diligence on the plan to verify that it will "work" under a wide variety of circumstances; (iii) verify that the vendor's plan is consistent with the customer's own business continuity plan; (iv) insist that the disaster recovery plan be attached as an exhibit to the contract, or at least referenced therein (if confidentiality concerns cannot be overcome); and (v) include contractual provisions addressing the evolution of the plan over time, the maintenance of the plan during the term of the relationship, and the implementation of the plan in the event of a "disaster." If the vendor does not have an adequate disaster recovery plan (and such failure does not disqualify the vendor), the customer should require the vendor to create, subject to the customer's approval, a disaster recovery plan that meets the customer's requirements.

In general, issues specific to the vendor's approach to disaster recovery on behalf of a particular customer will be divided into two categories, and addressed in one of two documents: in the agreement with the customer or in the vendor's disaster recovery plan itself. As with the customer's contingency plan, the vendor's disaster recovery plan, as applied to a particular customer, should include electronic movement of data to a safer environment on a regular basis. The plan should also include frequent testing of the disaster recovery plan by the vendor (perhaps with spot tests initiated by the customer), with re-tests in the event of failures. The customer should also consider requiring the vendor to maintain adequate backup or "mirror" facilities such that, if the vendor's facility goes down for certain environmental or other reasons, a backup facility can go live. In offshore arrangements, the backup facilities should be geographically disparate (in different countries, if possible). Other issues to be addressed in a customer's disaster recovery or contingency plan will include movement of affected employees and movement of operations to another country in the event of an outbreak of war or other similar unrest.

The legal agreement between the vendor and the customer will also address disaster recovery, generally in the context of those specific issues that are either unique between the customer and the vendor, or reflect specific commitments to the customer by the vendor (i.e., above those that the vendor may provide to its other customers in the normal course of business). For example, when the vendor has multiple customers, the

agreement may provide that the customer has either priority over other customers in the event of a disaster or has at least as great a level of priority as the vendor's other premium customers. The disaster recovery provision in the offshore outsourcing services agreement may also consider (1) access by the customer to insurance proceeds, and (2) whether foreign law restricts implementation of business continuity planning or disaster recovery procedures.

Force Majeure

Continuity of business is of heightened concern in some countries due to the possibility of disasters, war, geopolitical instability and other force majeure events. When negotiating the force majeure provision of an offshore outsourcing agreement, it is critical to read the list of events "defined" as force majeure. Consider whether, or not, the following are appropriate: (i) natural disasters (e.g., fire, flood, severe weather and earthquake), and likely and desired consequences; (ii) conflicts (e.g., war, terrorist attacks); (iii) governmental actions, whether initiated by the United States, the country in which the vendor or applicable facility is located, or a third country; (iv) changes in applicable laws that may frustrate or have an economic impact on the structure of the relationship (e.g., changes in tax laws); (v) employee/personnel actions, such as strikes, work stoppages or the threat thereof; or (vi) curtailment of transportation facilities preventing access or making it inadvisable to visit the vendor's facilities or for the vendor to perform its obligations. Of course, third party or resource failures that can be anticipated and planned for should be excluded from the list, unless the customer agrees otherwise (e.g., where the customer receives pricing concessions for agreeing to forego redundancy). Local law should also be consulted. For example, Article 94 of the Contract Law of the People's Republic of China provides that force majeure automatically gives the parties the right to terminate a contract.

The force majeure provision in an offshore outsourcing transaction must not conflict with the vendor's disaster recovery obligations or its obligation to maintain backup or "mirror" facilities (and implement other contingency plans). As discussed above, the provision should also tie in with the customer's right to terminate (without penalty) for force majeure-related downtime or other failure to provide services for a certain period of time. The vendor should be required to use reasonable/best efforts to work around and mitigate any force majeure event and the duration of any enforced delay should be limited.

Operational Oversight

It is generally not easy, and sometimes not even practical, to immediately terminate an offshore outsourcing relationship and shift operations either back in house, or to an alternate or backup vendor. Accordingly, the best approach is almost always to take steps to prevent the need to implement an exit strategy. Bad news is better than surprises! Customers are often surprised by the results afforded by:

- Regularly visiting the operations ... yes, in the jurisdiction in which they are being performed.
- Monitoring employee turnover rates and staffing.
- Establishing good governance structures ... and actually using them (i.e., planning for change ... and communicating effectively).
- Conducting on-going knowledge transfer ... certainly before you have to implement an exit strategy.
- Stress testing disaster recovery and relocation plans.

One possible structure for the governance model could include an offshore steering committee and an offshore program management office, with local monitoring and benchmarking. The offshore steering committee would: (a) define overall strategy; (b) develop internal support; and (c) oversee the customer's overall contingency plan. The offshore program management office would provide, among other things, oversight over the vendor's disaster recovery plan and an effective communications plan, including a clear check-in and reporting structure to contain any issues, a clear escalation process, and knowledge transfer procedures. From a business continuity perspective, the structure of the governance model should be designed to serve as an adequate early warning system for the customer.

Conclusion

Applying the customer's business continuity principles to an offshore outsourcing transaction is critical to understanding many of the business risks inherent in the transaction, including: (a) the potential for delay (even more likely and more extensive in an offshore transaction); (b) the potential for service disruption/lack of continuity; (c) the political implications affecting the relationship, directly or indirectly; and (d) whether certain events affect a single jurisdiction, or multiple jurisdictions. Understanding these business risks will enable the customer in an offshore outsourcing transaction to address them in its contingency plan, and to reflect that planning in the exit strategies that it employs with its various vendors, and in the disaster recovery plans that it requires of those vendors. Most importantly, however, by understanding the business continuity risks, the customer should seek to avoid as many potential disruptions as possible by putting in place appropriate operational oversight through a solid governance model.

Appendix B

Outsourcing Agreement “Sample” Table of Contents

1. PURPOSE AND STRUCTURE OF AGREEMENT
 - 1.1. Purpose of Agreement
 - 1.2. Structure of Agreement
 - 1.3. Supplier Parent Guaranty
2. TERM OF AGREEMENT
 - 2.1. Term of Agreement
 - 2.2. Extension of Services
3. THE SERVICES
 - 3.1. Obligation to Provide Services
 - 3.2. Compliance with Laws and Policies
 - 3.3. Procedures Manuals
 - 3.4. Services Performed by Customer or Third Parties
 - 3.5. Performance and Service Levels
 - 3.6. Disaster Recovery Services
 - 3.7. New Services
 - 3.8. Supplier to Provide and Manage Necessary Resources
 - 3.9. Functionality, Performance, Interoperability, etc.
 - 3.10. Reports
 - 3.11. Facilities
 - 3.12. Step-In Rights
4. CHARGES; NEW SERVICES; INVOICES; AND PAYMENTS
 - 4.1. Charges
 - 4.2. Taxes
 - 4.3. Invoices and Invoice Payment
 - 4.4. Benchmarking Process
 - 4.5. Service Level Credits
 - 4.6. Rights of Set-Off
 - 4.7. Disputed Charges/Credits
 - 4.8. Tariffs, Duties and Import/Export Compliance and Fees
 - 4.9. Changes in Customer Business
 - 4.10. Competitive Pricing

5. COVENANTS

- 5.1. Covenant of Cooperation and Good Faith
- 5.2. Services
- 5.3. Efficiency and Cost Effectiveness
- 5.4. Continuous Improvement
- 5.5. No Solicitation
- 5.6. Export; Regulatory Approvals
- 5.7. Viruses
- 5.8. Disabling Code
- 5.9. Services Not to be Withheld
- 5.10. Financial Covenants
- 5.11. Technology; Best Practices

6. REPRESENTATIONS AND WARRANTIES

- 6.1. Representations and Warranties of Customer
- 6.2. Representations and Warranties of Supplier
- 6.3. Pass-Through Warranties
- 6.4. Disclaimer

7. TRANSITION

- 7.1. Agreement on Transition Plan
- 7.2. Critical Transition Milestones
- 7.3. Conduct of the Transition
- 7.4. Customer Responsibility
- 7.5. Transition Charges
- 7.6. Transfer of Facilities and Assets
- 7.7. Affected Employees

8. GOVERNANCE; CONTRACT MANAGERS

- 8.1. Account Governance
- 8.2. Contract Managers

9. RELATIONSHIP PROTOCOLS

- 9.1. Personnel Resources
- 9.2. Use of Subcontractors
- 9.3. Contract Management
- 9.4. Required Consents
- 9.5. Change Control Procedures
- 9.6. Inspections and Audits

10. TECHNOLOGY; INTELLECTUAL PROPERTY RIGHTS

- 10.1. Technology
- 10.2. New Technology
- 10.3. Customer Software
- 10.4. Supplier Software
- 10.5. Source Code
- 10.6. Proprietary Rights

11. CONFIDENTIALITY AND DATA

- 11.1. Company Information
- 11.2. Obligations
- 11.3. Exclusions
- 11.4. Data Ownership; Customer Data
- 11.5. Security; Security Breach
- 11.6. Data Privacy
- 11.7. Limitation
- 11.8. Injunctive Relief

12. TERMINATION

- 12.1. Termination by Customer
- 12.2. Termination by Supplier
- 12.3. Termination Charges
- 12.4. Termination Assistance Services
- 12.5. Other Rights Upon Termination
- 12.6. Survival of Selected Provisions

13. LIABILITY

- 13.1. Liability Caps
- 13.2. Exclusions
- 13.3. Direct Damages
- 13.4. Remedies

14. INDEMNITIES

- 14.1. Indemnity by Supplier
- 14.2. Indemnity by Customer
- 14.3. Indemnification Procedures

15. INSURANCE AND RISK OF LOSS

- 15.1. Supplier Insurance
- 15.2. Risk of Property Loss
- 15.3. Contravention of Insurance

- 15.4. Waiver of Subrogation
- 16. DISPUTE RESOLUTION
 - 16.1. Disputes in General
 - 16.2. Continued Performance
 - 16.3. Exceptions to Dispute Resolution Procedures
 - 16.4. Governing Law
- 17. GENERAL
 - 17.1. Relationship of Parties
 - 17.2. Entire Agreement, Updates, Amendments and Modifications
 - 17.3. Force Majeure
 - 17.4. Waiver
 - 17.5. Severability
 - 17.6. Counterparts
 - 17.7. Binding Nature and Assignment
 - 17.8. Notices
 - 17.9. No Third Party Beneficiaries
 - 17.10. Rules of Construction
 - 17.11. Further Assurances
 - 17.12. Expenses