Business Continuity and Contingency Planning in Outsourcing

by James E. Meadows, *Culhane Meadows PLLC*

This practice note discusses business continuity and contingency planning in outsourcing transactions.

Companies typically consider outsourcing as a means to create flexibilities and opportunities that they may not otherwise be able to realize internally. However, to realize such benefits, the company 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, whether such changes are caused by unforeseen circumstances or otherwise.

A wide range of circumstances can impact business continuity. These circumstances can 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 with third parties, contractual or otherwise. Contingency planning to address direct circumstances seeks to anticipate possible, albeit unlikely, causes (e.g., force majeure events). This practice note focuses on contingency planning for circumstances involving third-party relationships, specifically outsourcing transactions that could adversely impact business continuity.

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

What follows is a roadmap for addressing the supplier situations that could impact customer business continuity and discussion of the benefits of combining a contractual exit strategy with proactive relationship building, as long as the customer has an adequate backup plan.

This approach focuses on:

- Joint contingency planning, attempting to address as many contingencies as possible
- Conducting diligence on the supplier's disaster recovery plan and managing the plan throughout the relationship
- Implementing strong governance mechanisms and an effective communication plan

By targeting these relationship elements, the customer can keep the supplier as focused on business continuity as the customer is itself.

Exit Strategies

Exit strategies generally define what happens, or is intended to happen, either upon the natural expiration of an outsourcing 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 outsourcing transaction for the purpose of terminating the relationship, certainly not the supplier. In general, it will be incumbent upon the customer to affirmatively raise the issue, because suppliers universally prefer long-term contracts to provide for more time to recover startup costs and maximize the total contract value. They also prefer long-term contracts because the longer a supplier's services are used the more dependent a customer becomes on the supplier. This is in contrast with the customer's desire for shorter terms to maintain flexibility and options.

Triggering Events

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 winddown or transition period). Triggering events often include:

- Varying types of breach by the supplier
- Bankruptcy or insolvency events (although bankruptcy as a trigger event will usually not be enforceable, or at least not in the U.S.)
- Force majeure events, with certain events triggering immediate exit, and other events triggering termination based upon the length of time incurred

Parties' Rights and Obligations

Once trigger events are established, the exit strategy will then address each party's rights and obligations associated with the termination before, during, and after. These include:

- **Customer Data or Information.** The supplier has an obligation to transfer any customer data or information obtained or stored by the supplier 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 or information transfers should be occurring regularly in an outsourcing relationship, whether transfers are to the customer or to a separate jurisdiction.
- **Transition Assistance Fees.** A means must be established to determine the fees for any transition assistance provided by the supplier. 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 baseline resources redirected to transition support (i.e., double billing). Finally, the transition assistance fees should contemplate the basis for termination; for example, no profit factor for transition assistance may be required where the customer is terminating for cause.
- **Continuation of Services.** A minimum period of time must be established in which the supplier will continue to provide the services at contract rates while the services are migrated back to the customer or to another supplier. During this same time period, provision should be made for knowledge transfer back to the customer (or its designee), to the extent that such knowledge transfer has not been happening throughout the term of the contract.
- **Necessary Employees.** If any supplier employees are necessary for the services, the customer should have the right to interview and hire these employees, although any such personnel decisions will necessarily implicate visa and Immigration and Naturalization (INS) compliance considerations.

- **Acquisition of Essential Assets.** If any equipment, software, or other technology is essential to the services, the customer should have the right to acquire these assets and the 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.

Issues to Consider

In formulating the exit strategy, the customer should also consider the following:

- Requiring the supplier's cooperation in the migration of the services to another service provider, perhaps even a competitor.
- The intricacies of unwinding the services associated with the particular infrastructure deployed by the supplier. It is easier to transition from a dedicated service than from one that is shared among multiple supplier clients.
- Unwinding the supplier's applicable subcontractor relationships. The customer should identify these during the diligence phase of the procurement process, noting potential termination impacts.
- Export and import regulations that may impact transition of operations and services back to the U.S. or to an alternative service provider.

Viability of the Exit Strategy

The concept of an exit strategy sounds useful and certainly is a logical topic for discussion in the negotiation of an outsourcing transaction. However, it is important to be aware that exit strategies often fail in an outsourcing context if adequate consideration is not given to what actually must happen upon termination. An exit strategy will only succeed if a robust backup plan is in effect, and that backup plan is 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 to complete all of the steps necessary to transition the call center away from the supplier in a relatively short timeframe. Does the customer have the requisite operational knowledge? This is not always a given if knowledge transfer has not been occurring continuously during the relationship. Does the transition include or require the supplier's employees? So, the ultimate question may be whether, or the extent to which, termination is a viable contingency plan.

Customer's Contingency Planning

Exit strategies in connection with individual outsourcing agreements only work when they are part of the customer's global business continuity plan. Here, we are assessing the customer's business continuity plan with respect to the specific function or process being outsourced. This plan will be implemented, in whole or in part, by the supplier, 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 supplier (i.e., multi-sourcing). 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 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) for handling contingencies—both internal teams within the customer organization and external teams through representatives of the applicable service providers and business partners—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 must be happening before the triggering event occurs; for example, ongoing knowledge transfer during the term of an outsourcing relationship. 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 typically also provide for the customer's right and ability to retrieve assets in the event of a service provider's insolvency or nonperformance. This right should exist even if claims or liens 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 outsourcing relationship may be made easier by consideration in the broader scope. In the event of two suppliers providing the same services to the customer, one supplier 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 supplier does best. However, often 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 suppliers) or may not be desirable from a business perspective. The traditional business reasons given for sole-sourcing include a) establishing a trusted relationship; b) volume benefits (e.g., cost, scale), and c) 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 supplier relationships for critical functions outsourced. In developing an outsourcing strategy, the customer should consider providers with geographically disparate facilities. At a minimum, the contract must provide the flexibility to establish such backup relationships, both from an affirmative (e.g., cooperation from the principal supplier) and negative (e.g., unrestricted right to engage third parties, or non-exclusivity) perspective. Of course, the supplier will usually 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.

Supplier's Disaster Recovery Plans

The customer can help to ensure that its outsourcing supplier is just as focused on business continuity as the customer is by doing the following:

- Ask to see the supplier's disaster recovery plan.
- Conduct extensive diligence on the plan to verify that it will work under a wide variety of circumstances.
- Verify that the supplier's plan is consistent with the customer's business continuity plan.
- 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.
- 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 supplier does not have an adequate disaster recovery plan, and such failure does not disqualify the supplier, the customer should require the supplier to create a disaster recovery plan that meets the customer's requirements, subject to the customer's approval.

Typically, issues specific to the supplier's approach to disaster recovery on behalf of a particular customer will be divided into two categories: (1) the supplier's plan to recover its own operation; and (2) its plan to recover the ability to resume performance of its contractual obligations. The issues will usually be addressed in one of two documents, either: (1) in the customer outsourcing agreement; or (2) in the supplier's own disaster recovery plan. The supplier's disaster recovery plan 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 supplier, perhaps with spot tests initiated by the customer, with re-tests in the event of failures. The customer should also consider requiring the supplier to maintain adequate backup or "mirror" facilities such that, if the supplier's facility goes down for certain environmental or other reasons, a backup facility can go live. In outsourcing 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 supplier and the customer will also address disaster recovery in the context of those specific issues that are either unique between the customer and the supplier, or reflect specific commitments to the customer by the supplier. These commitments would be above those that the supplier may provide to its other customers in the normal course of business. For example, when the supplier has multiple customers, the agreement may provide that a specific 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 supplier's other premium customers. The disaster recovery provision in the outsourcing services agreement may also consider access by the customer to insurance proceeds, and whether foreign law restricts implementation of business continuity planning or disaster recovery procedures.

Force Majeure Events

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 outsourcing agreement, it is critical to read the list of events included in the definition of force majeure. Consider whether or not the following are appropriate:

- Natural disasters (e.g., fire, flood, severe weather, and earthquake) and likely and desired consequences
- Conflicts (e.g., war or terrorist attacks)
- Governmental actions, whether initiated by the U.S., the country in which the supplier or applicable facility is located, or a third country
- Changes in applicable laws that may frustrate or have an economic impact on the structure of the relationship (e.g., changes in tax laws)
- Employee/personnel actions, such as strikes, work stoppages, or the threat thereof
- Curtailment of transportation facilities preventing access or making it inadvisable to visit the supplier's facilities or for the supplier to perform its obligations

Third-party or resource failures that can be anticipated and planned for should be excluded from the list, unless the customer agrees otherwise; for example, 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 outsourcing transaction must not conflict with the supplier'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 supplier 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 by Customer

It is usually not easy, and sometimes not even practical, to immediately terminate an outsourcing relationship and shift operations either back in house, or to an alternate or backup supplier. Accordingly, the best approach is almost always to take steps to prevent the need to implement an exit strategy, for example:

- Regularly visiting the operations 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 an exit strategy needs to be implemented
- Stress-testing disaster recovery and relocation plans

The selected structure for the outsourcing governance model could help to perform the above steps. For example, it could include an outsourcing agreement steering committee and a program management office, with local monitoring and benchmarking. The steering committee would define overall strategy, develop internal support, and oversee the customer's overall contingency plan. The program management office would provide, among other things, oversight over the supplier'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.

In conclusion, applying the customer's business continuity principles to an outsourcing transaction is critical to understanding many of the business risks inherent in the transaction, including: (a) the potential for delay, which is even more likely and more extensive in an outsourcing 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 outsourcing transaction to address them in its contingency plan, and to reflect that planning in the exit strategies that it employs with its various suppliers, and in the disaster recovery plans that it requires of those suppliers. Most importantly, 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.

For more related articles, visit *CounselLink COVID-19 Resource Center.*

LexisNexis®