

FOLEY EXECUTIVE BRIEFING SERIES



Strategic IT Contracting

Laying the Groundwork for Tomorrow's Success

Matt Karlyn
Foley & Lardner LLP
Boston

Stephen Riden
Foley & Lardner LLP
Boston



©2008 Foley & Lardner LLP • Attorney Advertising • Prior results do not guarantee a similar outcome • Models used are not clients, but may be representative of clients • 321 N. Clark Street, Suite 2800, Chicago, IL 60610 • 312.832.6500 • 07.3431



FOLEY EXECUTIVE BRIEFING SERIES

Learning Objectives

- Identify certain fundamentals in IT contracting
- Understand contract terms important in many information technology contracts
- Recognize issues particular to information security and how to protect your company's data and reduce your company's risk



©2009 Foley & Lardner LLP



Fundamentals



Economic Conflict in IT Transactions

- Vendor's economic objective is to maximize profit
- Customer's economic objective is to maximize service and reduce cost
- Effects
 - Drives divergent behavior
 - Places greater stress on agreement terms than most commercial relationships
- This economic conflict is augmented in an difficult economy



Capability Assessment

- A critical area of IT contracting that should remain unaffected by resource allocation
- Assessment phase builds the foundation for success
 - Benchmarking
 - Involve cross functional teams
 - Identify business objectives
 - Commit to a process and build the base case
 - SME review of statements of work and service levels
- Customer must know
 - What it wants to buy
 - What it seeks to achieve
 - How it wants to buy
 - The cost alternatives (including not doing the deal)
 - How it will manage the relationship
- Success begins with the initial data collection
 - Use to prepare RFP and evaluate responses
 - Fine-tune transaction process



Essential Considerations



Essential Considerations

- Definition of Services
- Business case / specifications
- License grant
- License fees
- Acceptance testing
- Warranties
- Limitation of liability
- Support
- Confidentiality
- Assignment
- Payment
- Contract administration
- Knowledge transfer
- Intellectual property
- Procure with a process



The Business Case

- Develop a plain English statement of your organization's business goals for implementing the solution
- The vendor agreements should be structured to establish the appropriate level of vendor accountability for achieving those goals



Services

- Everything is in approach
 - Even if a task is not identified, if it is necessary to complete a statement of work or comply with the agreement, it is part of the scope of the project
 - Opposite of vendor's approach (i.e., if it's not specified it will cost extra)
 - Middle ground → Identify excluded items in a schedule
 - Goal: Minimize surprises and cost increases associated with scope creep



Services: Suggestion

“Services” means the professional services to be performed by Vendor for Customer (a) as set forth in each of the statements of work, including, without limitation, preparation of the Deliverables and Work Product, (b) identified in the Agreement, (c) authorized by Customer to be provided by Vendor hereunder, and (d) any services, functions, or responsibilities not specifically described in this Agreement, but which are included as an inherent subtask of such services, are required for the proper performance and delivery of such services, or are otherwise necessary to comply with this Agreement, whether or not specifically set forth in (a), (b) or (c).



Specifications

- Most vendors warrant to the “documentation”
 - Vendors control the documentation
 - Documentation can change at any time (e.g., functionality “creep”)
- ASK: *Is specific functionality / interoperability required?*
- RFP and RFP response
- Tie-in warranties, business case and other of your business requirements
 - For example, consider a warranty that precludes any material reduction in functionality without a comparable replacement, unless reduction is mandated by law or agreed upon by the parties



License Grant

- Key term in any license agreement
- Types of licenses
 - Enterprise
 - Named user, concurrent user
 - Location
 - Hardware specific (server ID)
- Generally speaking, a broad license is desired
- Focus on who is the licensee



License Grant: Vendor Example

- *Subject to the terms and conditions of this Agreement, Vendor grants Customer a non-transferable, non-exclusive license to use the Software for its internal purposes.*



License Grant: Suggested Revision

- *Subject to the terms and conditions of this Agreement, Vendor grants to Customer a perpetual, non-exclusive license to use the Software for its business activities. Such business activities include, but are not limited to, the right of Customer's parents and their respective affiliates, subsidiaries, and joint venturers to access and use the Software. In addition, Customer may serve as a service bureau for the foregoing entities.*



License Fees

- Link to milestones in the implementation
- Minimum 20% holdback until “live”
- Beware of hidden third party license fees
 - Related issue: Third party license terms and conditions



Acceptance Testing

- Insist on some form of testing
- Define acceptance criteria
- Avoid automatic acceptance provisions
 - *Customer shall have 5 days to evaluate the software. If Customer fails to provide written notice of a defect within the 5 days, the software shall be deemed automatically and irrevocably accepted.*
- Link payments to acceptance
- Provide a remedy for failed acceptance
 - Acceptance cycle should end at some point



Warranties

- Avoid stock warranties of performance in accordance with the “published documentation”
 - “Published documentation is a moving target over which the vendor has complete, unilateral control
- What does the warranty really cover?
 - Frequently overlooked issue
 - Make sure performance warranties cover all of the following
 - Licensed software
 - Enhancement, releases and new versions
 - Documentation
 - Support and other professional services



Types of Warranties

- Performance (service levels, specifications)
- Intellectual property infringement
- Services
- Privacy laws and regulations
- Viruses and disabling mechanisms
- Open source

- *Be mindful of broad disclaimers that could override specific warranties (“as is, where is”)*



Warranties: Trends

- Integration Warranty
 - Software integration with all modules and the customer's existing system
- Open source software
 - Identify up front and list in an exhibit
 - Provide copies of applicable license agreements
 - Sufficient right to provide the open source software
 - Indemnity for breach of the warranty



Limitation of Liability

- What is excluded?
 - Consequential damages
 - Direct damages
 - Punitive damages
 - Liability arising out of indemnification obligations
 - Damages arising out of confidentiality or data security obligations
 - Assistance with respect to security breaches
 - Insured claims
 - Willful or intentional misconduct
- What is the liability cap?
 - Multiple of contract price
 - "Stair step" caps
 - Multiple caps for different types of damages
- Who is protected by the limitation of liability?



Support

- Fees are generally 12% to 20% of the yearly license fee
- What license fee is used as a base?
 - List
 - Fees actually paid
- Lock in fees for 3 to 5 years
 - Use a CPI or ECI adjustment



Confidentiality

- Is customer data at risk?
 - If yes
 - Warranty of compliance with (1) applicable state and federal laws and regulations, and (2) your company's privacy policy, processes and requirements
 - Security provisions
 - Exclude damages arising from a breach of the confidentiality and data security obligations from the limitation of liability (both for direct damages and any consequential damages exclusion)



Assignment

- Technology agreements, particularly license agreements, represent valuable assets to your company
 - Without the ability to assign those assets, at least in narrow circumstances, their value is substantially reduced
- Ability for transitioned entities to continue to use software for a limited time following termination and disentanglement/transition



Payment

- Should be structured to
 - Motivate performance
 - Assist project management
 - Protect against any agreement requiring significant payments despite dissatisfaction with vendor performance



Payment

- Determine if a fixed fee, time and materials, or hybrid payment method best promotes your business objectives
- Include performance incentives and credits
 - Payment withholding pending key milestone completion
 - Project cost overrun protections
 - *SOW hint: For fixed fee, cost overruns up to 10-15% are included in the fixed fee*



Fees

- Include “all fees” clause
 - *Except as set forth in this Section, or as otherwise agreed pursuant to Section 12 (Modification of Agreement), there are no other fees or costs to be paid by Customer under this Agreement.*
- Ensure that payment does not imply acceptance (and nullify acceptance opportunity)
 - *The making of any payment or payments by Customer, or the receipt thereof by Vendor, shall in no way affect the responsibility of Vendor to furnish the licensed software and services in accordance with this Agreement, and shall not imply acceptance by Customer of the licensed software or services or the waiver of any warranties or requirements of this Agreement.*



Material Breach

- Contract generally permit a party to terminate for the other party's "material" breach
- May be difficult to determine whether an event, a series of events, or a set of facts amounts to a material breach
 - Solution: Identify key scenarios and provide in contract that each such scenario constitutes a material breach
- Account for repeated small breaches



Source Code Escrow

- Escrow Agreement
 - Who is the escrow agent?
- Verification of deposit
- Notification of deposits in escrow account
- When must vendor make escrow deposits (initial and on-going)?
- Release triggers (next slide)
- Licensee's rights upon release
- Payment



Release Triggers

- Don't wait for bankruptcy
 - Failure to maintain and support licensed software
 - Significant decrease in capacity or quality of support
 - Failure to provide new releases that provide new functionality
 - Sunset of the product without suitable replacement



Force Majeure

- A force majeure event excuses a party's failure to perform
 - When failure results from some circumstance beyond a party's reasonable control (be careful of labor and supply shortages, failure of third party suppliers, and any act beyond the vendor's control)
 - Party's obligation to perform is deemed to be "suspended"
- Consider clause providing termination right if force majeure extends beyond a defined timeframe (e.g., 30 days)
- Ensure disaster recovery and business continuity obligations are precisely carved out of force majeure



Instead of Force Majeure

Vendor recognizes that Vendor provides Customer with services essential to its business operations, and that these services are of particular importance at the time of a riot, insurrection, civil unrest, natural disaster or similar event. Notwithstanding any other provision of this Agreement, full performance by Vendor during any riot, insurrection, civil unrest, natural disaster or similar event is not excused if such performance remains physically possible.



If Force Majeure is Required

Neither party shall be liable for, or be considered to be in breach of or default under this Agreement on account of, any delay or failure to perform as required by the Agreement if such delay or failure is caused by war, riot, insurrection, civil unrest, natural disaster or other act of God. Any party whose performance is delayed or prevented by any cause or condition within the purview of this Section shall promptly notify the other party thereof, the anticipated duration of the delay or prevention, and the action being taken to overcome or mitigate the delay or failure to perform. Notwithstanding the foregoing, under no circumstances shall any delay or failure to perform be excused or forgiven if the cause of the delay or failure could have been prevented or avoided by the exercise of all due diligence or if the party whose performance is delayed or prevented fails to use its best efforts to promptly overcome or mitigate the delay or failure to perform. Because of the importance to the Customer of the Licensed Software and the services to be provided under this Agreement, the parties acknowledge and agree that this provision shall be narrowly and restrictively construed to avoid excuse and favor performance of this Agreement.

Notwithstanding the foregoing, (1) Vendor shall not be relieved of responsibility under this Agreement unless it has deployed and is in compliance with its Disaster Recovery Plan, and (2) an event of force majeure will not relieve Vendor of its obligations under Section 14 (Data Backup and Disaster Plan; Business Continuity).



Contract Administration

- Personnel approval rights
 - Are personnel on-site?
 - Security and background checks
 - Compliance with policies and procedures
- Protect against project and cost risks resulting from key consultant turnover/transfer issues
 - Decide if a service level is appropriate
- Establish meaningful reporting mechanisms and processes
- Create an effective internal dispute resolution process
 - Informal dispute resolution coupled with a tiered escalation
- Control vendor subcontracting



Knowledge Transfer

- Do not underestimate the difficulty, value, or cost of successfully transferring necessary skills from the vendor to your organization
- Phase down vendor dependence during the course of implementation to test effectiveness of knowledge transfer and reduce cost



Protect Intellectual Property Rights

- The vendor team involved with your company's implementation is likely to be involved in similar tasks for one of your competitors in the future
 - Obtain ownership rights in all intellectual property used to develop the business processes upon which your organization depends
 - Protect your intellectual property and trade secrets (do not inadvertently waive trade secret protection)
 - Restrict key consultants from working similar engagements for your principal competitors for a period of time



Procure With A Process

- Be in a hurry to finish, not to start
- Know where you want to finish before you start
- Use the RFP as a tool to educate vendors regarding your company's business objectives and requirements
- Control the negotiation process
- Actively manage the relationship and contact compliance



Information Security



Common Risks

- Information Security
 - Two biggest mistakes
 - Focusing on technology
 - Failing to adequately address information security in third party relationships



Overview

- Security requires a unified approach
 - Security policies
 - Employee education
 - Use of technology (e.g., firewalls, encryption, intrusion detection systems)
 - Security audits
 - Addressing security in contracts with vendors and business partners



Types of Contracts / Relationships

- Any agreement under which a third party will have access to your company's
 - Network
 - Facilities
 - Data



What Are We Protecting?

- Confidential information
- Intellectual property
- Personally identifiable information
 - Healthcare – Health Insurance Portability and Accountability Act (HIPAA)
 - Financial – Gramm Leach Bliley Act (G-L-B)
 - State laws



Initial Due Diligence

- Make security part of the RFP process
- Develop an overall due diligence questionnaire
 - Security
 - Financial capability
 - Performance ability
 - Business continuity
- Put vendors on notice at the outset that security will be a critical part of the transaction



Contractual Protections

- NDA or confidentiality clause
 - Language should be broadly drafted to include all potential confidential information
- Warranties
 - Compliance with best industry practices
 - G-L-B compliance
 - HIPAA compliance
 - Compliance with your company's privacy policy and other privacy and security requirements, processes and policies



Contractual Protections

- General security obligations
 - Take all reasonable measures to secure and defend its systems and facilities from unauthorized access or intrusion
 - Periodically test systems and facilities for vulnerabilities
 - Immediate reporting of breaches
 - Joint security audits
- Specific information handling requirements



Contractual Protections

- Indemnity – protection from third party claims
 - Breach of confidentiality
 - Failure to comply with security requirements
- Exclusions from limitation of liability (both direct damage cap as well as exclusion of consequential damages)
 - Breach of requirements with respect to protection of confidential information and data security
 - Obligations arising out of vendor's obligation to indemnify customer under the agreement



Questions?

Matt Karlyn

Information Technology & Outsourcing Practice Group

(617) 502-3231

mkarlyn@foley.com

Stephen Riden

General Commercial Litigation

IP Litigation

(617) 342-4078

sriden@foley.com