CLOUD LEADERSHIP FORUM
Produced by IDC & IDG Enterprise
STRATEGIES FOR THE DYNAMIC ENTERPRISE

Cloud Contracting Workshop: New Challenges Arising in 2012

Michael Overly
Partner
Foley & Lardner LLP

Agenda

- Overview
- Reality check
- The BIG three
- Disaster Recovery
- Withholding of Service/Data
- Aggregated Data
- Bankruptcy/financial wherewithal
- Service level response time

Agenda

- Service level remedies
- Insurance
- Definition of Services
- Post-Execution Policing
- Negotiations

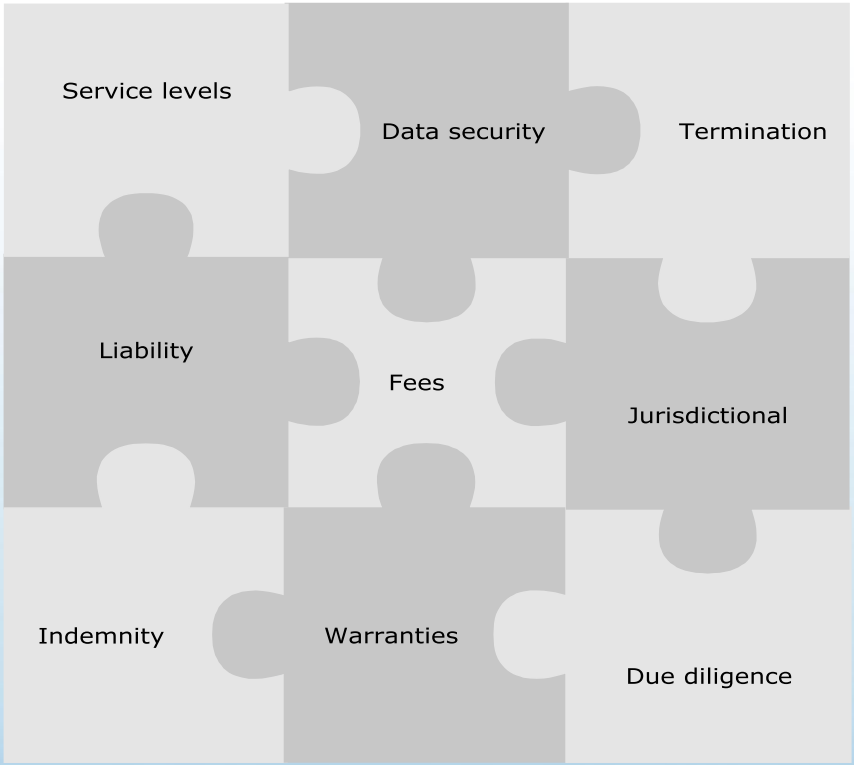
Reality Check

- Commodity services/pricing = inflexibility on contract terms
  - "*For the typical subscriber, however, a cloud's pricing policy and SLA are nonnegotiable*." NIST Draft Cloud Computing Synopsis and Recommendations
- Major vendors now presenting substantial, critical transactions "as-is"

Big Three

- Where in the world is my data?
  - Frequently no controls whatsoever
  - (Impossible) compliance burden shifted to customer
- "Contract float": SLAs, Service Description, Support Program
- New trend in liability

Legal Challenges of the Cloud



Service Availability – Disaster Recovery and Business Continuity

Scenario: Natural disaster is causing damage to the provider's data center

- Risk mitigation:
  - Include a provision requiring the provider to continue to make the services available, even in the event of a disaster, power outage, or similarly significant event.
  - Continuity of services should be provided through a secondary server, data center, or provider, as appropriate.
- Review any related provider policies and procedures
- Example:

Example: *Provider shall maintain and implement disaster recovery and avoidance procedures to ensure that the Services are not interrupted during any disaster. Provider shall provide Client with a copy of its current disaster recovery plan and all updates thereto during the Term. All requirements of this Agreement, including those relating to security, personnel due diligence, and training, shall apply to the Provider disaster recovery site.*

Service Availability – Disaster Recovery and Business Continuity

- Geographic separation
- Separate power grid
- Recovery point (acceptable data loss) and Recovery time (acceptable downtime) objectives
- Recovery site security
- Force majeure is not an exception to the SLA and DR/BCP
- How often is the DR/BCP Plan tested
  - Paper
  - Simulation
  - Parallel
  - Full cutover

Service Availability – Disaster Recovery and Business Continuity

- When was the DR/BCP plan last updated?
- Country-specific limitations
- Continuity trust/Direct contract
- Cost/benefit
  - Vendor's charging additional fees

Withholding of Services

Scenario: Provider is withholding service because of a fee dispute

- Include a provision prohibiting the provider's withholding of services
- Example:

Provided Client continues to timely make all undisputed payments, Provider warrants that during the Term of this Agreement it will not withhold Services provided hereunder, for any reason, including but not limited to a dispute between the parties arising under this Agreement, except as may be specifically authorized herein.

Withholding of Data

- Beware of vendors who withhold data on termination or in the event of a dispute
- Periodic copies
- Clear means and cost of obtaining data
- Data format
- Breach notification
- Fees

Aggregated Data

- Potential risks
- What does “aggregated” mean?
- Provided under a license
- As-is
- Indemnity from vendor

Electronic Evidence

- Vendor subpoenas without your knowledge
- Costs
- Cross-border implications
- Litigation holds

Bankruptcy; Financial Wherewithal

Scenario: Provider is closing its business because of financial difficulties

- Include a bankruptcy provision
  - provides the client the right to terminate the Agreement in the event of a provider bankruptcy
- Include a transition assistance services provision
  - requires the provider to assist in transition of the services to a 3rd party provider or to the client, in the event of expiration or termination of the Agreement
- However, once the provider has declared bankruptcy, Provider's ability to assist the client may be limited

Bankruptcy; Financial Wherewithal (cont'd.)

Scenario: Provider is closing its business because of financial difficulties

- If the client is not confident of the provider's financial stability, then consider adding a provision that enables the client to identify provider's financial issues *in advance*
  - Require the provider to deliver periodic reports on its financial condition
- Example:

Quarterly, during the Term, Provider shall provide Client with all information reasonably requested by Client to assess the overall financial strength and viability of Provider and Provider's ability to fully perform its obligations under this Agreement. In the event Client concludes that Provider does not have the financial wherewithal to fully perform as required hereunder, Client may terminate this Agreement without further obligation or liability by providing written notice to Provider.

Service Response Time Service Level

- Services that fail to provide timely responses to its users are effectively "unavailable"
- Therefore, include a service level that sets forth maximum response times for a customer's use of the Services
  - a specific service level target depends on the facts and circumstances in each case (e.g., transaction complexity, processing required, whether services are being accessed over an Internet connection or a leased line)
- Customer Satisfaction Surveys
- Example:

The average download time for each page of the Services, including all content contained therein, shall be within the lesser of (a) 0.5 seconds of the weekly Keynote Business 40 Internet Performance Index ("KB40") or (b) two (2) seconds. In the event the KB40 is discontinued, a successor index (such as average download times for all other customers of Provider) may be mutually agreed upon by the parties.

Service Levels – Simultaneous Visitors

- Does customer expect the services to support multiple simultaneous users?
- If so, include a service level explicitly specifying a requirement that aligns with customer's expectations

Service Levels – Problem Response Time and Resolution Time Service Levels

- Providers often include only a response time measurement, which typically falls short of what is necessary
  - Response Time
    - measures the time period from when the problem is reported to when the provider notifies the client and begins working to address the issue
- Also, include a resolution time measurement
  - Resolution Time
    - measures the time period from when the problem is reported to when the provider implements a fix or acceptable workaround

Service Levels – Remedies

- Credits
  - Typically, remedies for failure to hit a service level start out as credits towards the next period's service
- Right to Terminate
  - If repeated failure occurs, the client should have the right to terminate the agreement without penalty or having to wait for the current term to expire
- Example:

In the event the Services are not Available 99.99% of the time but are Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Client shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. In the event the Services are not Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Client shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. Additionally, in the event the Services are not Available 99.99% for (a) three (3) months consecutively or (b) any three (3) months during a consecutive six (6) month period, then, in addition to all other remedies available to Client, Client shall be entitled to terminate this Agreement upon written notice to Provider with no further liability, expense, or obligation to Provider.

Service Levels – Remedies

- SLA performance reporting
  - Beware shifting burden to customer
- Importance of remedy escalation/scaling
- Credits are not sole remedy
- Termination is frequently an unworkable protection

Notification of Security Issues

- Include requirement that if
  - a breach of security or confidentiality occurs, and
  - it requires notification to client's customers or employees under any privacy law,
  - then client should have sole control over the timing, content, and method of such notification.
- Also, if the provider is culpable for the breach, then the provider should be required to reimburse client for its reasonable out-of-pocket costs in providing the notification

Fees

- Client should have the ability to both add and remove IT resources, with a corresponding upward and downward adjustment of the service fees
  - Typically, a cloud computing service will be offered on a utility basis (i.e., “pay-as-you-go” or “pay-per-use” cost structure)
  - Negotiate rates for incremental and decremental use prior to signing
- All fees stated
  - Customer should make sure that the identified fees are inclusive of all potential revenue streams
- Fee cap
  - Customers should lock in any recurring fees for a period of time (1-3 years)
  - Thereafter, an escalator based on CPI (or other third party index) should apply

Insurance

- Client should carry Cyber-Liability Insurance
  - Insure against IT risks, such as the following:
    - unauthorized access to a computer system
  - theft or destruction of data
    - hacker attacks
    - denial of service attacks
    - malicious code
    - security breaches of personal information
    - violations of state and federal privacy regulations
- Provider should be required to carry Errors and Omissions Liability Insurance and Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access Insurance
  - Cover damages the client or others may suffer as a result of the provider's professional negligence and intentional acts by others (provider's employees, hackers, etc.)
  - Commercial General Liability Policy
    - It is critical that the client require the provider have more than just a commercial general liability policy (which may contain a professional services exclusion that precludes coverage for liability arising from IT services)

Definition of Services

- The definition of "Services" in a cloud computing agreement should be broadly worded to allow the client full use of the services.
- Example:

> *"Services" shall mean Provider's provision of software and infrastructure services described in Exhibit A (Services), and any other products, deliverables, and services to be provided by Provider to Client (i) described in a Statement of Work, (ii) identified in this Agreement, or (iii) otherwise necessary to comply with this Agreement, whether or not specifically set forth in (i) or (ii).*

- Customizations
  - Identify up front any additional customizations needed
  - Typically a cloud computing offering may have more limited customization options, so that the provider can more efficiently manage the services and provide a more scalable solution

Post-Execution – Ongoing Provider Assessment

- Establish a regular program of evaluating the provider's performance
  - Provider would be required to
    - supply the required information to assess the services,
    - notify the customer of any changes, and
    - provide any recommendations to improve the services
  - Allows the customer to
    - perform ongoing risk assessments during the term of the agreement, and
    - determine whether to continue the provider relationship

Negotiations

- Importance of checklists of key issues
- If customer has substantial negotiation leverage ..
  - Customer should seek to obtain the protections described
- If customer does not have such leverage …
  - Providers may be resistant to the protections described and any modification of its form contract provisions
  - May not be realistic to expect that customer can obtain all of the protections described

Negotiations

- If customer does not have such leverage …
  - Customer to evaluate the business risks – whether the services
    - support a critical business function
    - involve sensitive customer information
    - are customer facing
  - Walking away is an option
    - If not able to obtain the level of protection needed in the most significant areas of risk, then customer should consider walking away from the transaction
  - Walking away is not an acceptable option
    - If walking away is not an acceptable option, then customer needs to focus on risk mitigation (e.g., improved service level remedies and exit rights for service level failures, post-execution ongoing provider assessment, etc.)

Contact Information

Michael R. Overly, Esq. CISA, CISSP, CIPP, ISSMP, CRISC
Information Technology & Outsourcing
Foley & Lardner LLP
Tel: 213-972-4533
moverly@foley.com