Contracting With (or For) Application Service Providers

Thomas C. Carey
Bromberg & Sunstein LLP
Boston

Table of Contents

I. Glossary 1
II. The Industry 1
A. The Value Proposition 1
B. The Players Behind the Scenes 2
C. The Current Status of the Industry 2
D. Defining Customer Requirements 2
E. Ascertaining ASP Capabilities 3
III. Pricing Models 3
IV. Scope of Services 3
A. Applications Software 3
B. Custom Integration 4
C. Database Maintenance 4
D. Security 4
E. Help Desk 5
F. Change Management 5
G. Disaster Recovery 5
H. Purchase/Disposition of Legacy Equipment 5
I. Scalability 6
V. Service level parameters 6
A. Throughput 6
B. Availability (downtime) 6
C. Other issues: 6
VI. Warranties 6
VII. Intellectual Property Issues 7
VIII. Management 7
A. Steering Committee 7
B. Escalation Procedures 7
IX. Procedures at End of Relationship 7
X. Breach, Remedies 7
A. Penalties for down-time 7
B. Termination 7
C. Limitations of liabilities 8

I. Glossary

(a) An "ASP" deploys, hosts, and manages access to one or more packaged applications to multiple parties from a centrally managed facility. The applications are delivered over networks on a subscription basis. ASPs also provide, either directly or through third parties, other IT resources such as hardware, networking and operating software, support, maintenance and upgrades of applications.

(b) "Average Round-trip Latency": Total amount of time it takes for the first transmission to complete.

(c) "Average Round-trip Delay": Time it takes for subsequent transmissions, after the first transmission establishes the connection.

(d) "Defects Per Million": Minutes of downtime per million minutes of service.

(e) "Degraded Service": Not a full outage, but those periods when service is slower than contracted performance.

(f) "Impacted User Minutes": Number of affected users multiplied by the outage duration.

(g) "ISV" is an independent software vendor that may operate as, or partner with, an ASP.

(h) "Off-hours Problem Resolution": Target MTTR within each time zone noting off-hours during which resolution will take longer.

(i) "Outage": Change in performance keeping user groups from using the network. Can apply to any distinct category or all user groups.

(j) "Outage Duration": Total amount of time service is not available.

(k) "Total User Minutes": Total amount of time in a set period multiplied by the number of users being served.

(l) "Total Service Availability": Total impacted user minutes caused by all outages divided by the total user minutes.

(m) "Mean Time Between Failures (MTBF)": Average amount of time, typically in minutes or days, between outages**.**

(n) "Mean Time To Restore (MTTR)": Average amount of time, typically in minutes, it takes to restore service.

(o) "Trouble Rate": Frequency of how often technical support is required.

(p) "Repeat Trouble Rate": Frequency of times the same problem is reported.

(q) "Target Timeframe for Problem Resolution": Ideal times within each time zone that are preferable for problem resolution, inclusive of MTTR targets.

II. The Industry

A. The Value Proposition

ASPs try to deliver increased security, reliability and manageability, while lowering the total cost of ownership of an IT system to the customer. ASPs can provide frequent upgrades to software. Because IT is their core business, they can attract and retain highly competent IT professionals. By charging on a subscription basis, the ASP can reduce the up-front cost of software licenses. By making the same software

available to several customers, they can achieve economies of scale. Indeed, some studies have indicated that by leasing an application from an ASP, customers save between 33% and 53% over purchasing and managing the hardware and software for the application themselves. ASPs can also provide very fast time-to-market for companies needing to created new IT infrastructure quickly.

B. The Players Behind the Scenes

(a) The ISV (software provider whose application the ASP is offering)

(b) The access providers (telecoms, ISPs)

(c) Infrastructure operators (colocation and hosting providers, data storage providers)

(d) Infrastructure service providers make up the software and services layer of the Internet computing infrastructure, such as billing and metering, directory services or payment processing.

C. The Current Status of the Industry

ASPs began to develop as a business model in the latter half of the 1990s. Their first customers were the dot-coms, who could not take the time to build their own IT infrastructures. Now that the bloom is off the rose, ASPs need to prove their merit to more traditional businesses. Industry analysts predict both a high failure rate among existing ASPs and a high rate of growth for the industry as a whole.

Due Diligence

Before an ASP can begin to provide services to a customer, both parties must conduct due diligence of the other. The ASP must develop a good understanding of the customer's IT infrastructure and requirements, both present and future; and the customer must make certain that the ASP can perform as advertised. Outsourcing key functions to an ASP may involve the loss of in-house capabilities that will be difficult to replace if the ASP choice turns out to have been the wrong one.

D. Defining Customer Requirements

1. ASP Due Diligence: Identification of Customer Requirements

(a) Written description of functions to be set forth in statement of work

(b) Who prepares this analysis?

(i) The in-house IT department may lack enthusiasm for the assignment

(ii) The users may lack the expertise

(iii) An outside consultant may be necessary, or the ASP can provide the service on a consulting basis

2. IT usage

The ASP needs to determine what stress the customer will place on its IT system. In order to do this, the ASP must analyze the customer's current and prospective:

(a) Transaction volume;

(b) Processing time;

(c) Response time requirements; and

(d) Peak load requirements.

The ASP will not function in a vacuum. If it is taking over responsibility for key IT functions, it will need to know how to plan and coordinate system improvements, which are likely to be nearly continuous. This requires:

(e) Co-ordination required with IT to be continued in-house

(f) Current organization chart

3. User population

The ASP needs to understand the system users, whose use of the system may vary among subgroup. The ASP must understand:

(a) Characteristics of subgroups within user groups

(b) Do customers of the customer use the IT? Is this in the scope of services?

4. Legal due diligence

Are there existing service agreements that need termination in order to begin outsourcing? Can these terminations be effected without penalty? If not, who pays?

E. Ascertaining ASP Capabilities

1. Technical

(a) Availability of, expertise in, key software applications

(b) Hardware and communications capabilities (see sec. 3.1.2, "IT usage")

(c) Security systems

2. Legal

(a) Rights in Software

(i) Is ASP licensed to provide ASP services using third party software?

(ii) Internal software (source code escrow?)

(iii) Custom software for this project

(b) Other Proprietary Rights

III. Pricing Models

ASPs generally offer a subscription-based service. The pricing may vary from ASP to ASP, or be available in different flavors from the same ASP. Pricing may be based upon:

(a) Per month per User

(b) Transaction-based

(c) Layered (a la carte)

(d) Expect an escalator for long-term contracts to account for IT cost escalation

IV. Scope of Services

A. Applications Software

The ability of an ASP to offer cutting-edge applications software for the customer is a key to its appeal. This ability may stem from the ASP having developed proprietary software for a particular industry (e.g., biotechnology) or company function (e.g., HR); from its prior expertise in systems integration; or its having aggregated software from leading-edge ISVs.

1. Upgrades

(a) Frequency

(b) When performed (weekends?)

2. Recovery or reversal procedures if upgrade fails

The ASP outsourcing contract should, in its service level description, specify MTBF, MTTR, and acceptable levels of Degraded Service. Failure to adhere to the standards described in these service level specifications should result in penalty. Repeated failure should trigger customer termination right.

B. Custom Integration

The customer may require the integration of applications not currently in use by the ASP with others that the ASP does offer, or specially-tailored integration of applications then in the ASP's application suite, or special adaptation of a single software application. This system integration usually must be completed before the customer can begin to use the ASP's service.

C. Database Maintenance

The customer's data is paramount. The ASP will assume contractual responsibility for its proper maintenance, but may intend that this function, or some parts of it, will actually be performed by a third party. If the customer's confidence in the ASP depends upon the selection of the third party providing technical infrastructure, the customer should consider requiring continued use of that third party.

1. Redundancy

Mirrored hard drives may be necessary for data that cannot go off-line, even temporarily.

D. Security

1. Physical security

(i) Location of servers

Many ASPs offer extremely tight security measure protecting physical access to the customer's servers.

(ii) Backup procedures

The customer should specify the frequency of data back-up, and learn about the ASP's procedures for securing the back-ups against disaster. Are back-ups stored away from the servers? If so, how quickly can the data be restored from that remote location?

2. Firewalls

The customer can usually demand private leased lines, but may want to consider Internet-based access, which may be much less expensive. In that case, the ASP agreement should specify multiple firewalls and SSL (secure socket layer) encryption. The customer should ask the ASP for a security report or an audit from an accounting firm that details the ASP's security measures, and take the time to interview the ASP's security managers. Here are some questions to consider asking::

- Are you able to stop an attack and recover your infrastructure?
- What security assessment and integrity tools do you use and how often do you use them?
- What kinds of security controls do you use to protect customer data?

- How do you segregate clients sharing the same infrastructure?
- Which independent organization performs periodic auditing, testing and certification-or do you rely only on internal quality testing?
- What procedures do you use to authenticate users signing on to the system?
- What do you do toe keep viruses out of the system?
- How do you attempt to detect intruders?
- Do you engage a third party to test the security of the system?
- What reporting do you provide concerning breaches of security?

E. Help Desk

Since the ASP is providing the applications, it is logical for it to provide the help desk support for the end users. Sometimes this support is bifurcated, with in-house personnel providing "level 1" support, but having ASP resources available in case the problem is beyond the in-house expertise or relates to performance issues at the ASP end. The ASP Agreement should identify the scope of the helpdesk support being provided, and the hours of its availability. The agreement can also specify:

(a) Availability

(b) Response and resolution time

(c) Escalation process

(d) Identification of recurring/systemic errors

(e) Customer training requirements.

F. Change Management

The ASP should provide frequent upgrades and updates to the applications software. User training regarding enhancements and changes in functionality should be addressed in the ASP Agreement.

Either party may propose changes in the applications mix or utilization. Changes requiring significant additional programming and/or systems integration will require a change order, which needs to be approved by both parties, and specify any effects on the cost of the Agreement. Occasionally an ASP Agreement will provide a financial incentive to the ASP to come up with cost-saving changes to the customer's system.

G. Disaster Recovery

1. ASP disaster

The ASP and the customer should have a jointly-developed disaster recovery plan dealing with a disaster at the ASP's facilities. The ASP has to know which of the functions of the customer are most critical, and require restoration first.

2. Customer disaster

A disaster at the customer's facility is a matter over which the ASP has little control, and will generally constitute a force majeure event for the ASP Agreement. The customer must have a plan for dealing such an event. If the plan involves temporarily deploying an alternate network at a disaster recovery site, access to the ASP from that site must be in place.

H. Purchase/Disposition of Legacy Equipment

In some cases, the outsourcing that the ASP arrangement entails renders much of the hardware at the customer's site redundant. In some cases, the ASP can assume responsibility for purchasing or disposing of that equipment.

I. Scalability

If the customer need the capacity to grow very quickly, clearly the capacity of the ASP to handle such growth becomes and issue, and needs to be reviewed at the outset when the Agreement is in place. The cost of such growth, and the speed with which it can be accommodated, will be important.

V. Service level parameters

A. Throughput

If the communications relied upon is a leased line the ASP Agreement should specify the bandwidth being provided. If internet access is being used, then the customer needs to have the ASP specify the response time and throughput available to the customer at the ASP's facility.

B. Availability (downtime)

ASPs can provide redundant applications servers to ensure 24x7x365 application uptime.

1. Identify exclusions

(a) routine maintenance

(i) notification procedures

(b) customer-caused failures

(c) events beyond ASP's reasonable control

2. Different standards may apply to different aspects of service

(a) Communications

(i) expect 99.9% or better availability for leased lines

(ii) Mean time to repair: 4 hours industry average

(iii) for internet access, there are no standards applicable to packet/cell delays

(b) Distinguish between downtime and degraded service, with different penalties for the different problems.

C. Other issues:

(i) Average/maximum round trip latency

(ii) Time to full restoration

(iii) Time to full backup restoration

(iv) Tracking and Reporting of Adherence to agreed parameters

VI. Warranties

The customer should expect warranties for:

(a) ASP provision of applications without breach of third-party intellectual property rights; and

(b) Adherence to Service Level requirements for system availability, system response time, troubleshooting response time.

The ASP should also warrant that it will measure its own compliance with its service level parameters and report to customer regarding its performance.

VII. Intellectual Property Issues

(a) ASP's ownership of patents, trademarks, tradenames, trade secrets

(b) Customer's ownership of data

(c) Use of customer's name without prior consent

(d) License of ASP work product created during term of agreement after end of term

VIII. Management

A. Steering Committee

The agreement should require the establishment and maintenance of a steering committee to oversee the implementation and operation of the outsourcing relationship. The committee should meet regularly. Because considerable distances may separate the parties, telephonic meetings are usually acceptable.

B. Escalation Procedures

If the steering committee identified a problem that it is incapable of resolving, the ASP Agreement should provide for referral of the problem to senior executives of both parties.

IX. Procedures at End of Relationship

ASPs should present customers with clear exit strategies at the beginning of a relationship. The agreement should address whether the customer can purchase a software license at the end of the term and should require the ASP to cooperate in a crossover to a different ASP or in-house migration at the end of the term.

X. Breach, Remedies

A. Penalties for down-time

The Agreement should require service credits for measured amounts of downtime. Once an agreed-upon threshold of downtime is crossed, termination should be available. The customer should play close attention to the effect that any force majeure clause may have on this termination right.

B. Termination

1. Grounds for Termination

(a) Failure to meet agreed upon service level for a significant period of time (e.g., 3 months)

(b) Failure to pay

(c) Breach of confidentiality

(d) Unpermitted assignment of contract

(e) Insolvency

(f) Other "material" breach

(i) This provision may be unduly vague

(ii) Clearer examples of impermissible conduct (e.g., employee solicitation) should be substituted

2. Cure periods

(a) Different cure periods may be necessary for different breaches

(b) Some breaches may not be susceptible of cure. E.g., breach of confidentiality

C. Limitations of liabilities

The typical ASP agreement will attempt to limit liability to the amounts paid to the ASP under the agreement (perhaps over a 1-year period). The ASP Agreement proffered by the ASP will purport to rule our liability for consequential or special damages. While limitations and exclusions of this sort are typical in the IT industry, the customer may wish to resist these limitations in the event of damages arising out of:

- Infringement of intellectual property rights of third parties
- Breach of the customer's confidentiality
- Personal injury
- Willful misconduct