

July 2, 2003

Evaluating ASPs

Issues Agents Should Consider

By Agents Council for Technology

This agency checklist is designed to assist independent agencies in evaluating ASP opportunities by recommending a series of questions for agents to ask and then providing perspective on those questions. The checklist is divided into four major sections:

- I. Is an ASP Right for Me?
- II. Ascertaining the ASP's Performance & Service Commitments
- III. How are Problems Handled?
- IV. Implementing an ASP

I. Is an ASP Right for Me?

What is an ASP?

An ASP (application service provider) is any partner that provides offsite core technology solutions and support for your agency. ASPs extend way beyond online agency management systems. They can include other agency applications, such as rating, web sites, e-mail, office suites and specialized insurance software, and can be hosted by the vendor providing the software, a third party ASP vendor, or a carrier. This checklist is designed to assist the agent with respect to any of these types of ASPs.

When does an ASP solution make sense for my agency?

There is no cookie cutter response to this question. The answer depends very much on your analysis of the respective costs of outsourcing the particular technology versus managing it in-house, your access to technology expertise locally, and your interest in dedicating your time or other staff time to performing ongoing technology maintenance functions. At the end of the day, however, you do not want to move to a particular ASP unless you have a high degree of confidence that the ASP will provide your agency with a very secure, dependable, and responsive solution.

ASPs provide the following typical benefits:

- The ASP performs software, as well as hardware, upgrades and maintenance.
- Predictable/budgeted monthly subscription fee in lieu of large capital outlay upfront.
- Access to your application from any computer that has an Internet connection and the requisite client software.
- The ASP provides system securities, backups, redundancy and virus protection.

- Data is stored remotely.
- The ASP provides 24/7/365 server administration.
- Agency staff experience significant savings of time because many automation updating and maintenance functions are now done at the ASP level rather than locally. These functions, however, still must be performed on local equipment and networks and with regard to applications continuing to reside on local desktops or servers.

There are challenges, however, when an agency moves to an ASP, as outlined in the following questions, and these challenges must be addressed to the satisfaction of the agency.

What agency applications will the ASP handle and which will I still have to run and maintain locally?

In most cases when using an ASP, you still will have to maintain local servers, routers, networks, PCs and some applications, and continue to perform the necessary back-ups and updates for these applications. You will also need to provide security and virus protection throughout your local systems and back-up any data maintained on local desktops or servers. In many cases, the ASP solution will still win the cost-benefit analysis and make the local technology workload much more manageable. It is important to carefully think this issue through, however.

There are some third party hosting services emerging that will house not only the agency management system but also the additional third party software that the agency is likely to need, thereby potentially enabling an agency to move away from a server environment altogether.

Am I assured of the ASP's financial strength, dependability, and commitment to this offsite technology?

Agents should review the financial strength and track record of the vendor. Is being an ASP a core competency of this vendor, and is providing the ASP a major strategic direction for the vendor? In addition, what commitments is the vendor willing to give to maintain the particular ASP over time and to continue to make the necessary investments in technology to keep it "cutting edge"? As of this time, many vendors are implementing their software enhancements first in their ASP systems. It is critical for the agent to check references of current agent users of the ASP in order to evaluate dependability and responsiveness. In addition, the agent should review the vendor's audited financial statements in the same manner he or she would when entering a major business partnership with a third party. Also, if the ASP vendor uses a third party vendor to host the hardware and keep the servers up and running, the agent should reach the same comfortable level with regard to this third party vendor in terms of financial strength, dependability, and responsive service.

Does the ASP employ state of the art security, redundancy, back up, and catastrophe safeguards to fully protect my data and information?

Many agencies are attracted to ASPs because they are able to provide these protections more effectively than the agent can do locally. Agents should go over each of these areas with the ASP and assure themselves that the ASP does provide state of the art protections.

Does the ASP facilitate the agency's provision of technology to branch offices and the sharing of data among branch offices? Does the ASP facilitate agency employees accessing the agency's applications and data off site?

These are often stated benefits of using ASPs. Agencies should evaluate the particular benefits to their operations in these areas given their overall technology configurations.

Am I better off with an ASP if a catastrophe hits the agency?

If an agency's system goes down for whatever reason—catastrophe or otherwise-- the agency having an ASP can resume contact with it, provided the agent has access to a personal computer with an Internet connection. The catastrophe, however, could hit the ASP. The agency should assure itself that the ASP has built in adequate redundancy of systems to keep the ASP running from another location in this situation. As discussed at greater length in Section IV, the agency should also build in its own redundancy with respect to its high speed communications links in case a catastrophe hits one of those links. Agents are increasingly able to access the Internet and their ASP using a mobile phone or other personal digital device. Establishing this capability for the agency is an excellent catastrophe planning step.

What actual hardware and software does the ASP require to be maintained by the agency and how will the agency's third party software fit with the ASP?

Will the agency need to retool when it moves to the ASP? For example, will the ASP support the print drivers for the printers the agency has, or will the agency have to secure new printers? Will the agency's rating software continue to integrate with the ASP, or must the agency secure an updated version of this rating software? Will the agency's standalone life application continue to work with the ASP? If the ASP requires the latest version of Internet Explorer, will that work with the carriers' web sites that may be using an older version?

After doing an inventory of all of the software that the agency is using on its servers and various desktops, it needs to ascertain: (a) does this software continue to be important to the agency; (b) will it continue to work with the ASP; (c) will it continue to integrate with the ASP in either its current or an updated version; and (d) will the ASP host it? ASPs often provide agents with helpful information containing recommended local technology configurations and compatible software applications.

What restrictions does the ASP put on third party access to the system and on use of the data contained on the ASP?

Agents need to weigh the importance of restrictions that ASPs may put on the use of the agency's data that would not be present if the systems were in the agency. For example, does the ASP limit the agent's right to designate third parties to have access to the agency's data that is resident on the ASP? Can the agent designate clients to access the features available on the agent's web site such as quotes, billing information, payments, requests for changes, auto ids and certificates?

Similarly, can the agent continue to use other software programs that utilize the data on the ASP without the vendor's permission?

What have been the experiences of fellow agents using the ASP?

Has the ASP been reliable, cooperative, and flexible? What are the major benefits that these agencies have experienced from the ASP? What problems or limitations have these agencies experienced and how have they been worked out?

II. Ascertaining the ASP's Performance & Service Commitments

What are the ASP vendor's performance commitments and how does the vendor measure this performance? What recourse do I have if these performance commitments are not met?

To answer these questions, your agency should request the following from the ASP:

- Any generally recognized certifications and the requirements to obtain the certification.
- Server performance levels
- Maintenance steps to preserve server performance levels
- Server contingency plans for down-time
- Shared server versus Dedicated server
- Availability of data conversion programs should the ASP cease to exist or you switch applications or vendors
- Service growth plans (will they meet your future needs)
- Schedule of hardware maintenance and upgrades
- Schedule of application maintenance and upgrades
- Schedule of database backup
- Virus protection policies and procedures
- Security policies and procedures (Will they allow your security teams to test the security levels of the ASP?)
- Disaster recovery procedures
- Terms of service guarantee for term of contract

What is covered in the ASP's service agreement and what service guarantees are given?

A good ASP will not have any problems providing you with the following:

- A clear statement that you have sole and exclusive access to your data any time you desire.
- A statement that ensures your data will be used in accordance with your agency's privacy policy, including that the data will only be used to service the insured's business (not for testing or demonstrating the capability of system to potential new partners for the vendor).
- All standard hardware, application and database maintenance procedures and schedules, as well as security and virus procedures.
- Its daily backup services and disaster recovery procedures.
- The steps taken to ensure performance levels are maintained, as well as the steps and systems in place to minimize down-time.
- The ASP's plan for continued investment in its equipment upgrades, and its ability to sustain services through your growth.
- Whether your applications and data are stored on shared or dedicated servers.
- Service guarantees that the ASP will keep the application and hardware running the entire term of your agreement.
- Check the ASP's insurance coverage to see if it has a bond to handle "Interruption" in the event the ASP does not fulfill its service guarantees.

III. How Are Problems Handled?

What are the 24/7 procedures for ASP interruption?

Whom do you call if you have a problem with accessing your system after hours? Today, you can go reboot and/or reinstall your own system(s). With an ASP, you are completely dependent on someone competent being right there on-site and available immediately.

As discussed at greater length in Section IV, the agency's staff will need to be trained on trouble-shooting ASP problems and on whom to call to restore service.

If my ASP goes down, what is my back-up strategy to keep the agency functioning?

It is important for the agent to think through the possible scenarios, and how they will be handled. This will help in the ASP evaluation and negotiation process.

Frequently, the problem will not be with the ASP, but with the Internet Service Provider (ISP) which provides the agency's access to the Internet. Interruptions of service because of the ISP will not only affect the agency's access to the ASP but also to the carrier web sites. Issues to address with the ISP and Internet access are covered in the next Section.

In the event the ASP vendor goes under, exits the business, or fails to deliver, what are my contractual rights?

It is very important for the agent to have a clear contractual understanding as to what happens in the event the ASP fails to perform, goes bankrupt, or otherwise exits the business. If the vendor is acquired or otherwise sells the ASP, what assurances are contractually given to the agent to assure a continued professional approach by the new firm to hosting and continuously improving the ASP?

An agent should have the contractual right to compel the vendor to return the agency's data, including web site pages, as well as the necessary source code to permit the agent to read that data and convert it into other vendors' comparable applications, at the original ASP vendor's cost.

Agents should assure themselves that three clear protections are given by the ASP should problems arise. First, is a clear path provided for the agent to migrate back from the ASP solution to its in-house systems, and what is the cost to do that? Second, is the ASP's source code protected in escrow for the users should the ASP fail to perform in some way, and the source code is needed to read the agent's data housed in the ASP? Third, is the agency's exclusive right to its data housed by the ASP made crystal clear by contract and can this data be easily converted back to formats used by the major agency management systems?

Is my ownership of my data and other information clear and exclusive?

The contract with the ASP should make it very clear that the agency has exclusive ownership of its data and information and that the vendor will make it freely available to the agent at any time both during and following the relationship in a form that permits the agent to read that data and convert it into other vendors' comparable applications. The ASP should also make explicit that it will not disclose this data and information to any third party in individual or aggregate form, except to the extent the third party is carrying out a function for the ASP and agrees to hold the information confidential. Both the ASP and such third parties used for outsourcing should also demonstrate how they have instituted the proper safeguards to assure that this data is held securely and confidentially. Where the ASP is an insurance carrier, the same general principles should apply, and are encompassed within the Ownership of Expirations contractual provision, although the carrier also has rights to use the data to conduct its business. Specific carrier issues are covered in the next question.

In the event the agency merges or otherwise decides to change its system, the ASP vendor should provide the agency with a data transfer plan to allow the agency to transition to the new system over time without the need to stop, get the data, send it to the new vendor, convert it, and then go live on the new system.

If my ASP is an insurance carrier, what are my rights to get my policy information if there is a termination of the relationship?

Insurance carriers and their web sites can become an ASP for the agent, and agents are relying increasingly on electronic policy information housed at the company and accessible to the agent through the company web site or through the agency management system using real-time policy view or inquiry capabilities. Download remains very important to the agent, but sometimes particular data may not be available to the agent via download, particularly for certain commercial lines and specialized coverages. It is very important for the agent to establish an explicit understanding with the company that will allow the agent to have continued access to this electronic policy information following termination whether through the company system or through a CD provided by the company. Provision of this policy information by the company in a paper format is insufficient. See ACT's report "Turning off the Paper to Agents; The Key Responsibilities for Each of the Parties" for more detailed guidance.

What liability does the ASP have if data is "stolen" or "infected" or "lost"?

Is there any financial penalty for the ASP in these circumstances or for any other failure? If the agency's data or information is lost or corrupted by the ASP, does the ASP assume liability to pay for the restoration of that data and information? Are at least free services provided and fees returned when outages and other failures occur? These are important subjects for agent negotiation.

Does the ASP assume liability for an agency's business interruption in the event the ASP crashes for a period of time?

This is another point for the agency to consider in its contractual negotiations with an ASP.

Can the agency procure insurance to cover some of these risks arising out of ASP failures?

Does the agency's insurance provide it with any coverage in this situation? Can the agency procure systems interruption insurance to cover down time of the ASP; or if the ASP ultimately fails, the costs associated with getting the agency's data back online to service customers? Does the agency's E & O insurance respond if errors occur because of data display errors or security and privacy violations as the result of ASP or firewall problems?

Many unendorsed computer or EDP policies may not cover a loss of data, extra expense to recreate that data, or loss of business income since the data is stored on a non-owned hardware that is not located on an insured premises. It is recommended that you carefully review your insurance coverage.

IV. Implementing an ASP

Do I have a dependable high-speed communications link with the ASP supported by a financially strong and committed Internet Service Provider?

The more functions an agency handles on an ASP basis, the less the agency can do locally if the high speed communications link gets severed in some way. Maintaining a back-up dial up connection is the very minimum step an agency should take to protect itself. These connections, however, handle today's complex ASP transactions very slowly and inefficiently. ACT recommends that agencies maintain access to a back-up DSL or cable line to protect themselves against this risk. Often this back-up line will be maintained in the agency itself; however it could be at another location or in employees' homes. Access to the Internet and the ASP through wireless connections provided through PCs, mobile phones and other personal digital devices are becoming common and provide a good back-up connection as well an excellent communications vehicle in the event of a catastrophe. It is important for the agent to ascertain that the back-up communications link follows a different route than the regular ISP to provide for the maximum redundancy.

It is also advisable for the agency to keep a back-up router, because there can be delays in securing a replacement from the ISP provider.

Here are some good questions to ask your Internet Service Provider (ISP):

- Is the ISP a preferred partner to the phone company and in a position to get faster service than a business is likely to get going direct to the phone company?
- What are the procedures for handling spikes in service needs? For example, in the event of a major winter storm, hurricane or earthquake causing an increased demand on the ASP, does the Telecommunication provider have a plan to easily expand bandwidth?
- Is there a telecommunication ring in place so that interruption by one provider will be instantaneously replaced with service by another provider?
- What are the 24/7 procedures for ISP interruption? Whom do you call, and what is the service guarantee?
- Are there redundancies in the routes used by the ISP compared to the agency's back-up communications links to the Internet?

What training does the ASP provide agency employees so that they use this technology properly and fully understand its capabilities and limitations?

If not, how will agency employee training on the ASP be accomplished?

Agency employees need to be trained on trouble-shooting ASP problems and on whom to contact to restore service. If the ASP goes down, the employee should test whether it is an ISP problem or an ASP problem. If the employee can continue to navigate the rest of the Internet normally, then the problem is likely to be with the ASP. Agency employees

need to have a clear understanding about whom to call to restore service if it is an ISP, ASP, or local problem.

There also needs to be a clear understanding within the agency that the agency must continue to determine the security access levels permitted for particular staff even though most of the agency's technology is being housed off-site. In fact, since former employees can often access the ASP from any location with Internet access (rather than just in the agency location), it is critical for the agency to turn off the access of former employees immediately on all ASPs being used by the agency, including carrier sites.

As part of its savings in going to an ASP, an agency may decide to reduce its technology staff or consultant expense. There are still likely to be some local technology problems, however, so that the remaining staff may need to have greater technology training to make up for the lack of a technology consultant or "go to" person at the agency. The remaining agency staff also will need to continue to maintain and provide support for the local computers and connectivity network equipment.

Key issues for the agent to be aware of when transitioning from an in-house system to an ASP.

When agencies move to an ASP agency management system, they must go through a conversion process, just as they would do when moving to a new agency management system. Therefore, they will experience downtime while they perform the conversion steps of stopping their system, doing the back up, and sending it to the ASP. The vendors can often perform this process over a weekend, but the agent needs to get a clear understanding from the vendor regarding the steps and the downtime. Agents will need to physically deliver all of the third party application software to the ASP that the ASP will be hosting in addition to the agency management system.

As discussed in Section I, the agency needs to understand which of its hardware and software will work with the ASP, and what will need to be upgraded or replaced. The vendor's recommended agency technology configurations are very helpful to this process. The agency should test the ASP's print drivers to see if the agency's current printers will work. Some older desk printers might not be accessible through the ASP. Will the agency's rating software continue to integrate with the ASP, or must the agency secure a newer version of the rating software? The agency should go through a similar analysis with its other third party software.

This report was prepared by the ACT ASP Work Group

Richard Roy, Afni Insurance Services, Work Group Chairman
Peter Anderson, Anderson Insurance Services
Roger Barbe, Ohio Casualty
Amy Batson, Afni Insurance Services
Cal Durland, ACORD
Ed Higgins, Thousand Islands Agency

John Higginson, Applied Systems
Jon Jensen, Correll Insurance Group
Todd Mundhenke, Mundhenke Agency
Bob O'Connor, USI Hastings-Tapley
Roy Riley, Peel & Holland
Keith Savino, Warwick Resource Group
Bob Slocum, Slocum Insurance Agency
Jeff Yates, ACT Executive Director