

The Outsourcing Continuum



Contents...

The Outsourcing Continuum



2

2 The Outsourcing Continuum

Mike Scheuerman is an independent consultant with more than 26 years experience in strategic business planning and implementation. His experience from the computer room to the boardroom provides a broad spectrum view of how technology can be integrated with and contributes significantly to business strategy.

Mike can be reached at mike@scheuerman.org.



4

4 In-House Managed



6

6 Co-Location Managed



8

8 Fully Managed



10

10 Application Outsourcing



12

12 Making the Decision



14

14 Service Level Agreements



16

16 Certificates



18

18 Implementation

The Outsourcing Continuum

By Mike Scheuerman

There are a lot of people looking at outsourcing these days as a potential cost cutter. Let me say right up front that, more often than not, outsourcing won't save you a significant amount of money. More likely, what you will get is more value for the dollars spent.

The decision to outsource some or all of your IT infrastructure support is one that shouldn't be taken lightly, or without a significant amount of due diligence when considering which partner(s) to work with. Managing and maintaining the portions of your IT functions that are critical, but not strategic, requires considerable time and effort. You have to think about what elements of IT are contributing directly to your company's business strategies and which ones are providing "back office" type support.

Those that are back office functions are probably good candidates for outsourcing. Those that are strategic are ones that you want to give more time and resources. Even the strategic projects may have an element of outsourcing if you look closely at what items are one-shot tasks and which are ongoing.

Let's start by focusing primarily on IT infrastructure management and maintenance. The development of applications can be outsourced as well, but if you're developing applications, they are most likely competitive differentiators and you'll want to keep them close. If you happen to be developing an application that doesn't provide a competitive advantage you'd best look and see if it's worth doing at all.

When you start looking at IT infrastructure outsourcing you need to know that there is a continuum of services that range from very little outsourcing to lots of outsourcing.

There are three broad categories of outsourcing:

- In-House Managed
- Co-Location Managed
- Fully Managed

Each of these categories has both positive and negative aspects and each should be considered when deciding which outsourcing model works best for your organization.



In-House Managed

This category of outsourcing is probably the least costly because what you're paying for is remote expertise. You get the experts sitting off-site providing capability that you don't have. In this environment, your partner will have connections to your in-house systems. They can monitor and manage the systems as if they were located in your office. The great thing about this model is you don't have to hire the specialist you may need only occasionally. The cost of that expert

is spread across multiple clients and you're only paying for a tiny portion of the cost. The downside is you may not get quite the same level of response to requests for service that you might with a dedicated person. That can be mitigated by negotiating a service level agreement (SLA) that provides for the response time you believe you need it and can afford it. You also don't get some of the security of having your servers sitting in a hardened data center in the event of a disaster.

Co-Location Managed

This model is very similar to the in-house managed environment except the servers running your business are housed outside of your offices. The advantage is you will be more likely to have a robust physical facility with multiple sources of communication and power. That will ensure that your systems are available in the event of a disaster. The downside is you won't have quick, physical access to the machines.

You're also paying for the physical plant so it will be more costly than having the machines on site. However, odds are you won't have the same level of physical security and reliability on site so you have to weigh that risk against the cost of a better environment. You'll still have the cost of owning and maintaining the equipment. You'll also have to pay, as in the in-house model, for expertise to manage your systems.

Fully Managed

In this environment you don't own the servers and don't have to worry about whether they are up-to-date. You are paying for someone else to take on the technology refresh costs. You are also paying for the expertise to manage and monitor the systems. The systems you're using are housed in a risk managed environment with backup power and communications. Again, this is more expensive than the other models, but you have to weight that cost against the resources that you would be dedicating to the acquisition, management and maintenance of your systems.

Decisions, Decisions

In order to decide the right path for your organization, you have to understand the strategic business goals and how IT contributes to those plans. You also have to determine the risk that your company is willing to absorb and if outsourcing will mitigate or aggravate that risk.

Reviewing the offerings of multiple service providers can be daunting unless you have a good benchmark to measure those services against. You'll need to negotiate an SLA that protects against poor service. All of these tasks take time and effort to do right but, if well done, they can lead to a far stronger IT contribution to the company's business.

As we continue, we'll examine more of the details of how each of these outsourcing models work and what you need to do to determine what is the best plan of action for you and your company. ■

In-House Managed

This category of outsourcing is probably the least costly because what you're paying for is remote expertise. In this model, you own the equipment and physical environment it sits in. What you don't have is a bunch of hardware engineers on your staff. You get those experts sitting at your partner's site.

In this environment, your partner will have connections to your on-site systems. They will monitor and manage your systems as if they were located in your office. The great thing about this model is you don't have to hire the specialist you may only need occasionally. The cost of that expert is spread across multiple clients and you're only paying for a tiny portion of the cost.

The downside is you may not get quite the same level of response to requests for service that you might with a dedicated resource. You don't get to run down the hall to IT when you have a problem. This can be mitigated by negotiating a service level agreement (SLA) that provides for the response time you need and can afford.

The scope of work covered by under the SLA should include the following network administration tasks:

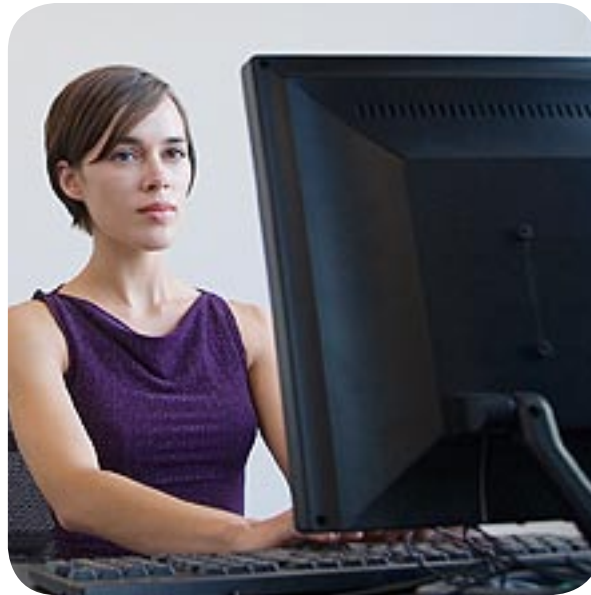
- Adding users and establishing network permissions for users
- Deleting users and denying user access to network
- Deploying patches and security updates
- Maintaining domain structure and related tasks, virus updates, user security, user lock down, and migration

In the event of a network failure, the partner will provide all labor required to restore the network to proper operation. Action will be taken immediately to regain operational status within a defined time (e.g., four hours). Labor to assure that

the network is secure and stable will be provided.

This includes:

- Providing regularly scheduled on-site appointments to ensure the network is operating at a satisfactory performance level
- Ensuring that back-up operations are completed on a regular basis
- Examining daily back-ups and clear the event logs on a regular basis
- Ensuring that anti-virus definitions are up to date
- Installing all security updates and OEM patches
- Installing all software upgrades when they are available and appropriate for the site



Response via e-mail or phone within a defined time (e.g., 30 minutes) of being contacted.

This includes:

- Assisting employees in further identification and isolation of the problem
- Working with employee(s) to prioritize the problem and set realistic expectations for resolution
- Providing remote, technical support to servers, desktop users, and remote users
- Problems that affect a single employee should be repaired within one business day

Monitoring software on all servers. This includes:

- Set meaningful thresholds to monitor CPU loads, disk space utilization, and RAM
- Measure the performance of network against thresholds and set automated alerts to maximize server uptime
- Provide reports to management that will help achieve a higher ROI on hardware

Meeting with the management periodically to make recommendations that will accommodate the proper size and configuration of the network components based upon industry best practices for the size and type of business.

This includes:

- Provide recommendations based upon the business expansion or contraction
- Advise on emerging technologies that affect the business. Likewise, advise on technology obsolescence
- Providing limited training to help the users advance in their daily tasks including assisting users through remote access by shadowing users during a remote terminal services session

Acting as a single point of contact for vendors that impact the network. This includes:

- Consulting with telephony specialists as related to network configuration
- Consulting with software and hardware OEM vendors as needed
- Assessing and reporting the operational status of the equipment periodically (at least once per month)
- Creating and maintaining network diagrams and documentation
- Notifying via e-mail, phone or fax of all repairs, changes, and reconfigurations made to the equipment
- Maintaining a communications infrastructure capable of complying with this scope of work

What You Won't Get

You don't get the security of having your servers sitting in a hardened data center in the event of a disaster. You still have to pay for the power and physical improvements to accommodate the equipment in your office. You still have to negotiate with the communications company to get the appropriate bandwidth for your needs and arrange to have it installed. You'll still have to buy the hardware and pay for the installation and maintenance. You still have to buy the operating

system software and any applications you want to use. You'll still have to make sure you have someone on staff that has responsibility for managing the relationship with your service provider and making sure that you get what you're paying for. And, finally, you'll still be responsible for making sure that the backups of your data and systems are done regularly. Somebody will have to put the tapes in the tape drive and rotate them to off-site storage. You will have to develop, maintain, and test a Business Continuity Plan.

What it Costs

The costs for this kind of outsourcing are usually based on the number and type of machines that are being supported. For example, if you have six servers, 50 desktops, 20 laptops, and a handful of PDAs, your costs might look like those in the following table.

As you can see, this is less than the annual cost for a single

Qty	Monthly Fee	Hardware Type	Amount
50 x	\$30.00 ea	Windows™ Desktops	\$1,500.00
20 x	\$40.00 ea	Windows™ Laptops	\$800.00
6 x	\$20.00 ea	PDA's and Handhelds	\$120.00
6 x	\$300.00 ea	Windows™ Servers	\$1,800.00
76 x	\$6.00 ea	PC Maintenance, proactive monitoring, alerting, self-healing, patch management and asset management	\$456.00
Total Monthly Fees			\$4,676.00

good network administrator and you get much more value for your dollars. With in-house managed outsourcing, there will still be plenty for your IT staff to do, but they will be focused on adding business value not maintaining the power plant. It also means that you may need to have a different kind of person in IT—one who understands your business and how technology enhances and supports that business.

In the next article, we'll examine more of the details of the co-location outsourcing model. ■

Co-Location Managed

This category of outsourcing adds “ping, power, and pipe” services to the in-house managed model. The service provider offers co-location by providing space, power, and a link to the Internet for their customers’ servers. They do not perform maintenance or troubleshooting. They only provide a rack to house the servers and a repetitive test to make sure the servers are running. The customer will be notified if the server fails. Known as a “ping-power-pipe” arrangement, “ping” means sending a packet to the server to see if it responds, “power” is electricity, and “pipe” is the line to the Internet.

In this model, you own the equipment but the physical environment it sits in is owned and operated by the service provider. You don’t have staff of hardware engineers and you don’t have a computer room to manage or pay for. The advantage is you will be more likely to have a robust physical facility with multiple sources of communication and power. That will help ensure that your systems are available in the event of a disaster. The downside is that you won’t have quick, physical access to the machines.

You’re also paying for the physical plant so it will be more costly than having the machines on-site. However the odds are you won’t have the same level of physical security and reliability on-site so you have to weigh that risk against the cost of a better environment. You’ll still have the cost of owning and maintaining the equipment. You’ll also have to pay, as in the in-house model, for expertise to manage your systems.

What You Should Get

With co-location you get the security of having your servers sitting in a hardened data center in the event of a disaster. In this model you are paying for several items:

A place to put your equipment (rack space):

- Connectivity from your office to the data center
- Connectivity from the data center to the Internet
- Reliable power and communications infrastructure

Each of these items has numerous options that you’ll have to sort through to get the appropriate configuration.

Racks: Rack space is measured in 1.75-in. high Rack Units (RU or U). The height of your equipment determines the amount of rack space you’ll need. A typical rack will hold 40U, so if you have six servers each 2U high, then you’ll probably need at least one-third of a rack.



Connectivity: Connectivity to your network and to the Internet is what’s needed to make sure that you can communicate with your servers. These connections will come in a variety of bandwidths ranging from the equivalent of DSL speeds up to the highest speeds available. You will have to decide what amount of data you are going to move between your office and the servers to determine how much bandwidth you need to pay for. If you have heavy traffic to a server-based application then you’ll want to have more data bandwidth available on that side of

the equation. The same is true of the Internet connection: if you have a lot of data coming in from the Internet (such as an e-commerce application), then you’ll want more bandwidth to accommodate that.

If you’re just doing normal office Internet surfing you’ll probably need less Internet bandwidth. You should purchase the amount of bandwidth that you use on an average basis. There will be a surcharge for using more than that, but that can be mitigated by making sure that the surcharge is based on a 95 percent measurement of sustained usage. If you push a lot of data to your servers occasionally, that won’t cost anything extra.

Power: The power in the data center should be backed up by an uninterruptible power supply (UPS) to ensure that in the event of a power outage, the equipment will continue to run long enough to enable a clean shutdown. Additionally, you'll want to make sure that the data center has a generator available to provide power in the event of an extended power outage.

You should also check on the fuel resupply contract that the data center operator has for its generator(s). You'll want a fuel resupply contract that ensures the generator will continue to operate over several days just in case the "ice storm of the century" takes out the power lines.

Communications: Communications between your office and the data center are crucial to a successful outsourcing project. You will want to make sure that the data center has multiple carriers supplying communications. The data center should have very large bandwidth data lines coming in from those carriers, again to make sure that you don't have a bottleneck communicating with your servers.

You'll also want to know that those communication lines come into the data center from different directions (just in case a backhoe breaks a line). The data center won't commit to a response time minimum between your office and the data center since they can't control all the active elements of the network. However, once the data has reached the data center you should have a committed minimum latency within the data center to ensure that slow response is not the data center's fault.

Service Level Agreement

The scope of services covered by under the SLA should include the following:

Bandwidth Availability Commitment:

- At least 99.99% of the time the contracted bandwidth should be available
- A service charge credit if that level of availability is not met

Network Availability Commitment including:

- At least 99.99% availability of the service provider network
- A service charge credit if that level of availability is not met

Latency Commitment:

- Service provider network will have an average round trip packet transit time within the data center backbone network of a defined amount. Typically this will be 70ms or less

- A service charge credit if that level of latency is not met
- A commitment to maintaining a communications infrastructure capable of complying with this scope of services

What You Won't Get

You'll have to buy the hardware and pay for the installation and maintenance. You have to buy the operating system software and any applications you want to use. You'll have to make sure that you have someone on staff that has responsibility for managing the relationship with your service provider and making sure that you get what you're paying for. You will also have to have someone managing and maintaining the systems. This could be your own staff or you could combine this model with the in-house managed model to have a third party manage the servers.

You'll be responsible for making sure that the backups of your data and systems are done regularly. Somebody will have to put the tapes in the tape drive and rotate them to off-site storage. You will have to develop, maintain, and test a Business Continuity Plan.

Costs

The costs for this kind of outsourcing are usually based on physical space that you occupy in the data center and the communications bandwidth you need plus any extras you might want. For example, if you have six servers running general applications and moderate bandwidth needs, your costs might look like those in the following table:

Service	Setup	Monthly
1 / 2 Rack (20 RU) 2x20 Amp power circuits	\$250	\$600
1.0 mbps bandwidth (up to 10 mbps in bursts)		\$250
Backup Tape Rotation	\$75	\$200
Total Fees	\$325	\$1,050

This is probably less than the annual cost for a rack, power, and the air conditioner and communications costs from a local carrier. You get more value for your dollars because you can be assured that your systems are sitting in an environment that is better protected than in your office.

With co-location outsourcing, there is still the issue of managing the applications. You can have your IT staff do that or you could outsource that, as well. One thing they won't be doing is maintaining the power plant.

In the next article, we'll examine more of the details of the fully managed outsourcing model. ■

Fully Managed

In the fully managed model, you don't own the equipment. You are paying for someone else to take on the costs for technology refresh and the expertise to manage and monitor the systems.

The physical environment is owned and operated by the service provider. You don't have a staff of hardware engineers and you don't have a computer room to manage or pay for. You don't have to worry about upgrading your machines or the environment in which they reside. They will be in a robust physical facility with multiple sources of communication and power.

You don't really care about the equipment, because it belongs to someone else and it's their problem to worry about keeping it running. You are paying for a certain level of service as defined in the service level agreement (SLA). As long as the service levels are met you really don't care how it gets done. This is more expensive than other models, but you have to weigh that cost against the resources that you would be dedicating to the acquisition, housing, management, and maintenance of your systems.

With managed services you get the security of having your servers sitting in a hardened data center in the event of a disaster. In this model you are paying a level of service that you and the provider will define as a part of the negotiation and configuration discussions.

Typically you'll pay for:

- A defined number of servers
- Connectivity from your office to the servers
- Reliable power and communications infrastructure
- Horizontal software applications, e.g., operating systems, database engine
- Regular updates to the software and hardware
- 24x7 monitoring of systems with alerts to let you know if there's something amiss.

- Regular reports on service levels

Servers: The servers may be physical or virtual servers. More and more service providers are using virtual server environments. This trend will likely continue and you needn't be concerned with the physical arrangement of the equipment. If you have a small number of applications you may only need one or two physical servers running multiple virtual environments.



Connectivity: As in the co-location model, connectivity to your office network and to the Internet is what's needed to make sure that you can access the servers that are doing the work. There are myriad communication speeds ranging from the equivalent of DSL speeds up to the highest speeds available. You will have to work with your service provider to decide how much data you are going to move between your office and the servers.

This will determine how much bandwidth you need. If you have heavy traffic to a server-based application then you'll want to have more data bandwidth available on that side of the equation.

If you have a lot of data coming in an e-commerce application, then you'll want more bandwidth to accommodate that. If you're just doing normal office Internet surfing you'll probably need less bandwidth.

You should purchase the amount of bandwidth that you use on an average basis. There will be a surcharge for using more than that, but that can be mitigated by making sure that the surcharge is based on a 95% measurement of sustained usage. If you push a lot of data to your servers occasionally, that won't cost anything extra.

Horizontal Software: Horizontal software is the software that is needed across all application platforms and systems.

This includes the operating system with on-going deployment of patches and updates to current version as released from vendor. If you are using a database like Oracle or MS-SQL, the service provider should have a certified expert on staff to manage and maintain the database engine. You shouldn't expect to have support for any applications that run using that database.

24x7 Monitoring: Monitoring will include a long list of things that need to be watched. This will typically be done from a 24x7x365 network operations center (NOC).

Items that will be monitored will include:

- Hardware, e.g., memory usage, disk space, CPU utilization, etc.
- Communication ports
- System logs
- Horizontal software, i.e., is it running?

Reports: You should get at least an annual hardware and software performance report to let you know what has been done to maintain the agreed to service levels. You'll want to get a security and vulnerability report at least twice a year to make sure that the systems you're using are safe and secure. On a quarterly basis you'll want to see reports on operating system and horizontal application performance tuning, hardware maintenance including firmware and BIOS updates and physical support tasks that were done.

Power and Comms: As in the co-location model, the power in the data center should be backed up by an uninterruptible power supply (UPS) to ensure that in the event of a power outage. The service provider should have at least two communications services providers to ensure that the loss of any one communication channel doesn't significantly impact you.

SLA: The scope of services covered by under the SLA should include a response commitment. This includes:

- A commitment to respond to any failure of the operating system, server infrastructure, or service provider network within a negotiated time frame (2 to 4 hours)
- A service charge credit if that level of response is not met

Bandwidth availability commitment:

- At least 99.99% of the time the contracted bandwidth should be available
- A service charge credit if that level of availability is not met.

Network availability commitment:

- At least 99.99% availability of the service provider network
- A service charge credit if that level of availability is not met
- A commitment to maintaining a hardware infrastructure capable of complying with the negotiated scope of services.

What You Won't Get

With this model, you get a lot, but you will have to buy and maintain any applications you want to use. This could be done by your own staff or you could have the software vendor support those systems if they provide that kind of service. You'll have to make sure that you have someone on staff that has responsibility for managing the relationship with your service provider and making sure that you get what you're paying for. You will have to develop, maintain, and test a business continuity plan or disaster recovery plan.

Costs

The costs for this kind of outsourcing vary widely depending on what services you are buying. The pricing is based on the service provider's cost of system acquisition and maintenance, as well as the cost of hiring the experts needed to maintain those systems. For example, if you have six physical servers running general applications and moderate bandwidth needs, your costs might look like those in the following table.

Service	Quantity	Setup	Monthly
Windows 2000/2003 Dedicated Server	6	\$3,000	\$4,500
1.0 mbps bandwidth (up to 10 mbps in bursts)		\$0	\$250
Managed Firewall	1	\$250	\$250
Ethernet Switch	1	\$200	\$300
Backup Tape Rotation		\$75	\$200
Total Fees		\$3,525	\$5,500

To determine if this is cost effective you'll need to sit down with the guys in finance and figure out the cost of acquisition and depreciation. Don't forget to figure in the cost of power for the systems and the air conditioner and communications costs from a local carrier. You also have to include in your calculations the costs of the staff to monitor systems 24x7x365 as well as the staff costs for engineers to maintain and monitor the systems.

You get more value for your dollars because you don't have to worry about buying and maintaining servers. You also get the security of knowing that someone is watch your systems around the clock to make sure that they're up and running, doing what you need to get done. ■

Application Outsourcing

In addition to the infrastructure outsourcing we've been discussing thus far, there is also an opportunity to outsource selected applications that are important to the company but not strategic. Let's consider all the business functions that are common to many businesses, for example, your e-mail server.

Modern business relies on e-mail to do business every day, so it's very important that you have an e-mail connection. But do you really want to dedicate internal resources to managing and maintaining an e-mail server? There are literally dozens of companies that will provide you with an e-mail service that in many ways may be superior to what you have now.

What about your CRM function? It's important for the salesforce to be able to track their customers and sales pipeline, but building and maintaining a CRM server takes resources away from focusing on the really important applications that provide your business with a competitive advantage. Let's take a look at an e-mail example and see what the analysis looks like. There are two types of e-mail outsourcing available, Web-only and hosted server. Each of these has its strengths and weaknesses, but generally they will do the job pretty effectively for very little cost. As in all outsourcing, you'll need to make sure that the service level agreement (SLA) meets the needs of your company.

What you should get from both types of service providers are:

- Large mailboxes (2+ GB)
- Large e-mail attachments (at least 20 MB)
- Virus protection
- Spam filtering
- Secure access to e-mail
- E-mail client access via standard access protocols.

What you should get from hosted-server service providers are:

- Locally installed e-mail client (e.g., Outlook, Eudora, Scribe, etc.)
- Web access to e-mail.

The mailbox and attachment size will determine how much data can be immediately accessible in the user mailbox.



Many users of business e-mail are used to having very large inboxes because they rarely clean them out. So, the larger the mailbox the more e-mails can be retained. E-mail attachments seem to be getting bigger and bigger, so make sure that you aren't too limited when it comes to the size of the documents you attach to an e-mail. This can be very frustrating for some users if they just want to quickly share a document with a colleague.

Security

There are literally hundreds of thousands of malicious software types (viruses, trojans, spybots, etc.) running around the Internet. Unfortunately many of them are transmitted via e-mail, so you want to make sure that you have all the protection you can get to avoid compromising your internal networks. Unfortunately, the majority of e-mail traffic today is junk mail from spammers, so you'll want any service provider to stop that spam before it reaches your users' inboxes.

Another great feature of e-mail is the ability to encrypt sensitive information to ensure that it doesn't get read by unauthorized people. You'll also want secure encrypted access to your e-mail, wherever it is stored.

Access Protocols

There are a couple of standard e-mail protocols, POP3 (post office protocol 3) and IMAP (Internet message access protocol), that you will want a service provider to make available. This will allow your users to get their e-mail delivered to the standard e-mail client that you have installed on their systems. Typically, the service provider will give you a set of easy to follow instructions on how to set up an e-mail client like Outlook or Eudora to access e-mail stored on their servers.

What you won't get are unlimited mailboxes. You will have to train your users on how to keep their mail organized and their e-mail boxes down to a reasonable size. This is going to be tough for some folks (you know who they are) because they don't ever clean out their inbox. With the basic e-mail service you typically won't get mobile e-mail support for your smart phones and PDAs, either. That, in most cases, is an extra cost item.

The costs for e-mail services have a fairly wide range, but on average you should be able to get basic e-mail service for around \$10 per user per month. There are lots of options available to customize the service to your needs. It's a bit like a Chinese menu and each item adds a little more the total bill.

App Outsourcing in General

There a number of companies offering software subscriptions today. Everything from CRM to ERP systems can be obtained from an outsourcing service provider. These subscription-based services are sold under various labels (SaaS, software as a service, cloud computing, etc).

In a software subscription environment the focus of your company stays on the core business and not on the technology that enables the business. When you have someone else worrying about the nuances of accounts receivable processing you can devote more resources to generating the business that creates the accounts receivable. Many companies already do this when they outsource their payroll processing. They don't worry about whether the tax tables are up-to-date; they just worry about whether their employees are productive.

The time and effort involved in maintaining and updating generic business applications software goes away. Someone who is far more knowledgeable about the subtleties of a

particular business application will update the software without your in-house staff doing all the research to determine whether this is a good update or not. You don't have to worry about whether you need to spend money on a new server because the old one ran out of gas the software subscription vendor takes care of that as a part of the subscription.

You also don't have to worry about running the backup every day, because your provider will do that for you. From a business continuity perspective you're in much better shape since you can run the subscription business process from just about any computer. So, if a disaster strikes, your normal business processes can be up and running again as fast as you can run down to the local Best Buy and get a new machine and get online.

You can count on what it will cost to run that part of your business. You know exactly how much it costs you to run your general ledger or accounts payable or CRM. Under a licensed model, there are a lot of hidden costs that you don't know about or track so you don't really know other than the cost of the software, what it costs you to run those systems.

The downside is these offerings are still in their infancy so they may not be as flexible as they will be in the future. They aren't fully business hardened yet so there are going to be problems that crop up that you don't see in a licensed software package. The upside is that the provider's business is dependent on a stable service offering and they will throw every resource they have at resolving the problem quickly.

It will take a lot more due diligence to determine what vendor can provide you with the stable, secure, reliable business process functions. You won't be able to walk into the local software store and pick up a software package and walk out. Of course, when you do that today you have to go back to your office and figure out how to install it and get trained on how to use it.

The range of outsourcing options is growing daily so you'll want to keep your eyes open for opportunities within your company to consider outsourcing not only your infrastructure but also the basic business applications that are essential to business operation but are not critical to your business strategy. ■

Making the Decision

O utsourcing is a business decision that weighs the strategic plans for the company against the resources required to accomplish those goals. Determining the appropriate resource allotment for any particular goal involves considering both tangible and intangible costs to achieve the goal. For example, if your goal is to increase market share in a particular market segment, then you may commit more resources to the development of product enhancements that appeal to that market segment as well as increasing the marketing and sales resources that target that market.

In this case, you may have your internal staff direct the efforts of outside organizations to print and distribute new sales literature. You might also have an outside engineering firm work on the product enhancement under the direction of your product development management team. In each of these cases, you have a tangible cost for getting a particular piece of work accomplished. You also have an intangible cost related to the quality and timeliness of getting the job done. Of course, you can do all the work internally, but unless you have the right people with the right skills, your product quality and time to market may suffer. The intangible cost would be a missed market window.

The same kind of logic applies to outsourcing your IT infrastructure. Are you going to commit your IT resources to building and maintaining servers and networks or do you want them working on things that help the company meet its strategic goals? The answer to that question obviously has to do with why you are in business. Most companies are not in the business of providing IT infrastructure support. IT is simply a means to an end. Why not consider letting someone else do the work of supporting your networks and focus your

IT staff on business process enhancement and managing the outsourced work?

Questions you should ask when making the outsourcing decision:

- What is IT doing today in support of the corporate business strategy?
- Does the IT organization provide good business value or is it just keeping the lights on?
- What does IT cost today?
- Will outsourcing save money or provide more value for the dollars spent?



Business Strategy

Here the goal is to move toward an environment where infrastructure is supported by outside service experts while maintaining the business critical elements in-house. If, for example, you are deploying a new custom software application that will do great things for the business there are several elements of the project that might be outsourced. You might contract to have some of the programming

done by outside vendors, while maintaining project management control in-house. You could have the servers that the application runs on managed by an outside firm. You might even think about building the entire application on a platform such as the ones provided by Salesforce.com, Google, or Amazon.

The point is that your technology strategy should be focused on providing business value rather than infrastructure management.

Developing a strategy that puts critical elements of technology in the hands of others is a little scary. That kind of strategy

requires that your IT team develop a new set of management skills to ensure you find and manage the right partners. The technology team will have to gain more insight into the company's business processes and strategy, a greater understanding of the service levels needed, and a better way to perform vendor due diligence investigations.

The IT team is no longer strictly in charge of technology, but rather of ensuring that everyone in the company can get their job done. The competitive edge is not in the technology but the application of the technology in innovative, cost-effective ways.

IT Value vs. Cost

Making the switch to concentrating on the "Information" in Information Technology will be challenging for many of today's IT managers. They have always worried about the speeds and feeds and less about how the equipment under their control provides good value. Infrastructure management is necessary but not sufficient to provide business users and managers with the information they need to make critical business decisions each and every day.

The challenge to implementing this model is developing a true cost model of IT services so a reasonable comparison of costs and goals can be achieved.

Today, the cost of IT is calculated largely on the personnel costs and the capital costs of the assets that IT provides. In truth, the opportunity costs of not providing more effective utilization of people in the business units is unaccounted for (this assumes, of course, that IT does improve effectiveness). The cost of not being able to determine the state of the business in a more timely way is left out of the equation. And the cost of decisions being made with incomplete information is missed. The cost of system down time is also largely ignored.

If, for example, you had 40 people making \$25/hour and your systems were down just 0.5% of the time, it would cost you \$43,800 per year. Putting real dollar figures to intangible items is difficult, but the risk to the business is too high not to make an educated estimate.

Most business managers never think about the technology they use every day and how lost they would be without it. They

are concerned about the cost of the technology and what it lacks. These are real concerns. But, if business management can step back and think about IT as a utility they will begin to see that trying to keep the IT infrastructure running is like buying and maintaining your own power plant. You wouldn't do that because you can't justify the cost.

You use the power to run your business and focus on the things that make your business successful, you don't worry about buying coal to keep the power plant running. IT should be viewed the same way, it is an information utility. The real value comes from the information that is generated by the plant, not in the electricity flowing through the wires.

Outsourcing Value

Step back and look at what you're doing. By now you've outsourced your payroll so people get paid the right amount on time. You have outsourced your sales process management to somebody like Salesforce.com or Microsoft Office Live. Why aren't you outsourcing the other pieces of business process, like support, to somebody who knows what they're doing? They have the experienced staff to solve problems quickly. They can help you put together a disaster recovery plan. They can help you protect your valuable information from theft and hackers. Your IT staff with

limited knowledge and resources cannot do that no matter how smart or hard working they are. Get them some help.

One caveat, don't outsource and forget. You need to manage an outsourcing partner just as you would an employee. It's an important part of your company and you don't want to just let somebody else make all the decisions when they don't sit in your seat. Will outsourcing save you money? Maybe not directly, but when you calculate the lost opportunity costs of inefficient business processes, late development projects, time lost due to lack of skill or time or knowledge, the outsourcing decision will look a lot better. ■

Major Outsourcing Models

	In-house Managed	Co-location Managed	Fully Managed	SaaS
Where is equipment physically located	All the servers are installed in-house	All the servers and communications gear are located at the data center	All the servers and communications gear are located at the data center	All the servers, communications gear and applications are located at the data center
Cost	Capital expenditure outlay for equipment plus a monthly fee	Capital expenditure outlay for equipment, a monthly fee, and either internal or external management resource costs	Monthly fee	Monthly subscriber fee
Need for internal IT support	Depends on service level and desktop support requirements	Depends on service level and desktop support requirements	Depends on service level and desktop support requirements	Depends on service level and desktop support requirements
Owner of equipment	Company	Company	Either	Service Provider
Responsibility for management of servers	Management services provider	Either	Hosting provider	Service Provider
Responsibility for management of operating system and software	Management services provider	Either	Hosting provider	Service Provider
Responsibility for maintenance and administration	Management services provider	Either	Hosting provider	Service Provider

Service Level Agreements

When you put a crucial portion of your company's service into the hands of a third-party service provider, you lose some control over the operational aspects. You are relying on the partner to meet your expectations for quality of service. In order to protect yourself from some of that risk, there are two service level metrics that you want to address in the contract: uptime and response time.

Uptime

Uptime refers to the amount of time a system is available for use. It's calculated as a percentage of the total available time. If you have 99% uptime for the month, the system was available for use 712.8 hours out of the total 720 hours in a 30-day period. To get a good feel for what uptime levels are appropriate for your company, look at the current levels of service you are providing to your customers. For example, if you are providing online service processing only during the hours your offices is open, and you intend to continue with that practice, then you probably don't need 24x7 service levels but you do want to have the system up and functional when you're actively taking providing support to your customers.

The service level you want for the hours you are supporting customers is very high, whereas the uptime for the rest of the day can be very low. Typically, you will want to get agreement for uptime to be in excess of 98% for operational use hours. That number will exclude any scheduled maintenance downtime. That means if the system is scheduled to be down for maintenance, that time will be excluded from the available time in the uptime calculations.

Response time refers to the amount of time that it takes to get an answer back from the system once the user has en-

tered data. It is typically measured in seconds from the time the user presses the submit key until data is returned to the screen. There can be a wide range of response times depending on the work the system is required to do to come up with an answer and the complexity of the network.

You want to determine what an average response time should be and build that into your SLA. For example, for a system that is doing a simple calculation and is directly connected to

the user terminal, you would expect to see a response in less than two seconds. For a system that is doing a complex task like scoring a loan application and the user is connected via the Internet, you might expect to see response times of as much as 45 seconds.

The primary issue here is productivity. If an application is too slow, the user will not get as much accomplished in the same period as they would with a more responsive product. They will also get impatient and perceive it as a poor system. Not a good customer service situation.

Enforcement

On the enforcement side of the SLA, you have a couple of options. If the provider fails to perform at the desired level, you can ask for a refund of monthly fees or you can terminate the contract. Both of these options are valid separately, however, the combination is even better. If your uptimes don't meet the SLA levels you may want to consider getting a refund of a portion of the monthly fees you're paying for the system. For example you might want to get a 10% refund for every percentage point under the agreed to uptime. If the system was unavailable on an unscheduled basis for 96% of the month and you had a 98% SLA, you would get a 20% refund on your monthly services fees. This, again, is a productivity issue for your company. If the application wasn't available then you weren't able to do business and thus there



is some loss for which you should be compensated.

To address chronic uptime/response problems, you can build in a contract termination clause if uptime and/or response time levels are not acceptable over a defined period. Typically, that period would be a fixed time frame of three to six months. You can also use chronic problems six months out of 12 to trigger a contract termination.

You will want to be careful about invoking this part of the SLA, because it means that you will have to find another vendor and retrain your staff, which can be very time consuming and expensive. You will have to determine if the cost of changing is better than frustrating them continuously by having a system that is not up and usable.

Problem Resolution Procedures

The second part of an SLA addresses how problems are resolved when things go wrong. It may be a critical problem where the system is totally down or just a minor inconvenience. In either case, you will want to know what is being done to fix the problem. You should have your vendor provide you with a set of priority definitions as they apply to problems, i.e., what does critical mean, what is severe, etc. Along with

those definitions you should also get a resolution time frame, who to contact to report a problem and how often you will be updated on progress toward a solution to the problem.

If the problem is not solved in the agreed upon time frame, what do you do? The SLA should contain an escalation procedure including contact information.

The last thing contained in a good SLA is a list of the reports that you can expect to receive that tells you how well the vendor is providing the service levels. These may be just a couple of e-mail reports on a monthly basis or they may be detailed analysis of every aspect of the service. It doesn't really matter how you receive the information, just make sure that you get something that lets you determine if you've gotten the levels of service you expect and are paying for.

Most vendors will be willing to supply you with a SLA. This is one way they can compete in the marketplace and can point to the SLA as their commitment to their customers. If a vendor isn't willing to supply most or all of the service levels and problem resolution procedures, you may have to consider whether their support structure is able to provide you with the kind of service you can rely on to support your business. ■

Certificates

Now that you've decided that outsourcing is an option that you want to pursue, you'll need to find a service provider that will meet your companies needs. There a number of factors that need to be considered when choosing a service provider.

First and foremost, the question needs to be asked: Do you want a partner or a vendor? This question is tough to answer, because in the strictest sense, it is always a vendor relationship. Sometimes it takes time to grow a vendor relationship into a partnership. You can get a sense of how a service vendor interacts with their clients by talking to some of their reference clients.

Questions that you should ask are:

- Does this vendor work with you to develop a strategy for the success of your organization?
- Does the vendor have established processes for reviewing and upgrading the services provided?
- Is the service process flexible enough to provide for special needs that your organization may have or does it just offer a menu of services with no provision for unique requirements?
- Does the vendor provide a service level that matches your organization's internal service level commitments?
- Is there a written service level agreement (SLA)? The SLA should address regular communications on a proactive basis. Simply reacting is not good enough anymore.
- Is the vendor committed to maintaining certifications that ensure that you and your organization comply with the various regulatory bodies' requirements and that your data is held securely? For example, do they support your Sarbanes-Oxley requirements?

Since I have addressed many on the other questions in previous articles, this article is going to focus on which certifications you should keep in mind when hiring a partner and why.

Certifications

When you review the qualifications of a service provider you need to consider what, if any, certifications are needed for your industry as well as general certifications that cross industry lines. For most companies two important certifications are required. Particularly important for public companies is the SAS-70 audit because it is one of the foundations for Sarbanes-Oxley regulations. In addition, many service vendors are coming to realize that the information technology infrastructure library (ITIL) is a way to provide consistently superior service to their clients. Although there is currently no ITIL compliant certification for organizations, those that have implemented ITIL processes may be able to achieve compliance with and seek certification under ISO/IEC 20000, the international standard for IT service management.



If you happen to be in a business that accepts or handles credit card information, you will want to know that your service provider complies with the payment card industry data security standard (PCI DSS). This standard is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment.

SAS-70

SAS-70 sets out the detailed guidelines and the standards of reporting on the effectiveness and adequacy of internal control procedures and activities by the service organization.

SAS-70 requires an independent auditor or auditing firm to examine the implemented controls in a service organization and report on the effectiveness and adequacy of the control activities, procedures and objectives in place in the service organization. The SAS-70 audit report includes the auditor's opinion on the effectiveness of the controls in use as practiced in the organization under audit.

There are two different types of SAS-70 reports. The first type, commonly referred to as Type I, includes an opinion written by the service auditor. Type I reports describe the degree to which the service organization fairly represents its services in regard to controls that have been implemented.

Type II reports are similar to Type I, however, an additional section is added. Type II reports are more complete, because the auditor gives an opinion on how effective the controls operated during the defined period of the review. Type I only lists the controls, but Type II tests the efficacy of these controls to provide reasonable assurance that they are working correctly.

ITIL

ITIL is published in a series of books, each of which cover a wide range of IT management topics. ITIL gives a detailed description of the best practices of a number of important IT processes with comprehensive checklists, tasks and procedures that can be tailored to any IT organization.

ITIL is in its third revision now after its initial development in the late 1980s. ITIL v3, published in May 2007, is comprised of five key volumes: Service Strategy, Service Design,

Service Transition, Service Operation, and Continual Service Improvement.

While ITIL covers a wide range of topics on IT service management, the most widely used portion of the library is the service management set. The service management set covers topics such as service desk operation, incident management, software asset management, change management and service level management. All of these are important areas that, if implemented properly, can provide a much more stable and secure technology environment.

Any service vendor that is committed to providing ITIL training and process development will more likely to be focused on providing a superior level of service to you and your organization.

PCI DSS

PCI applies to organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any card holder data. If any customer of your company ever pays you directly using a credit card or debit card, then the PCI DSS requirements apply.

Finding a service partner that fits your organization's needs is challenging. Talking to their current clients will give you a sense of how well the vendors works with others and how they might fit your organization. When you talk to the management staff, see if they are eager to understand your business so they can provide services that your business needs to grow and prosper. ■

Implementation

Once you have decided to outsource your infrastructure support and have done your due diligence selecting a service provider, it is time to implement the plan. There are several steps that you will go through with your vendor to ensure that you get what you expected when you signed the outsourcing contract.

1. Establish and implement standards
2. Consult on technology usage
3. Design a system to support business initiatives
4. Procure equipment to support the design
5. Implement a new infrastructure

Establish the Base

The establishment of solid foundation is critical to future growth. Your service provider will work with you to implement the basic security, system maintenance and help desk support that you will need to support the implementation of systems that contribute to business growth and value.

During this period, standards will be put in place. Things like disparate operating system versions (e.g., Windows98, Windows 2000, Windows XP, Windows Vista) will be whittled down to one easily maintainable version. Multiple versions of office productivity software (word processors, spreadsheets, e-mail clients, etc.) will likewise be pared down to a common application set. Security measures such as firewalls, anti-virus, and anti-spam software will be configured, tested, and installed.

Monitoring software will be installed to watch the critical components of the hardware and software. Alert levels will be established to determine if something is going awry, it can be fixed before it causes a failure. Computers that are unable

to run the chosen operating system and applications will be replaced.

A new helpdesk system for reporting problems will be established and employees will be trained on how to use that system. This system will enable your service provider to begin to build up a knowledge base of the kinds of problems that occur most often. With that information, the vendor's technical personnel will be able to identify the root causes of those recurring problems and fix them. That will lead to a more stable working environment for all employees and allow them to be more productive.



Technology Usage

While the base infrastructure is being revamped to stabilize it, you should expect to spend a significant amount of time with your service provider partner determining what exactly you want your technology to deliver. This will allow them to design a future infrastructure that will support the initiatives that are a part of your business strategy.

It also provides you with a view of which initiatives are easy to implement, which are dependent on other applications or hardware and which are going to require significant investment.

During this stage of the outsourcing cycle, you will be presented with multiple options for implementing any particular business initiative. Your service provider will be able to explain the pros and cons of each of these options so you can make a rational decision on which would best meet your business goals.

Design and Procure

Once you have decided which initiatives are most important to your business. Your service provider in conjunction with your

internal staff will set about building the detail design for the systems that will be needed to implement those initiatives.

It is critical that your internal staff be a part of the design team. Only your staff knows in detail what kind of work needs to be accomplished to successfully implement any new business initiative.

During this stage the service provider can be of great assistance in recommending technology solutions, but they can't know your business as well as you do, so don't expect them to design a system that will work just right for you if you don't give them guidance. Your partner will probably be able to procure the right equipment and services more cost-effectively than you can, so let them do that, but negotiate a budget with them and expect them to meet it.

New System Implementation

Once you have designed and procured a new system, it is time to implement. A set of steps similar to the original base establishment begins. Any new equipment that is needed will be put into place; employees will be trained on the new business processes and software; the helpdesk will begin building up a knowledgebase on the new systems and applications. Because you established a solid base to work with during

your initial implementation phase, you won't have to worry about breaking the business processes you have in place already.

Summary

As you may have surmised by now, all of this takes a significant amount of time and effort. You should allow at least three months before you can expect things to get better. In most cases, it will take six months to a year before you will begin to see real improvements in productivity.

When you started on your journey to outsourcing, you had expectations that you would never have to worry about your technology infrastructure again. Now that it is real, you will find that for the most part those expectations have been met. You now think/worry more about how you can use the application of the technology to provide your business with competitive advantage. You worry more about whether your business processes are the most efficient, and how they can take on more growth.

These are the things that you should worry about. Leave the technology worries to those who are experts in technology. Your worries should be about how to grow your business and use the technology to enable and enhance that growth. ■