

# MANAGED SERVICES

---

## A How-To Guide

- What Are Managed Services
- When and Where to Use Them
- Acquiring Services
- Defining Service-Level Agreements
- Managing Service Performance
- Getting the Most From Your Provider

For additional copies or to download this  
How-To Guide, please visit:  
**[www.govtech.com/managedservices](http://www.govtech.com/managedservices)**

© 2009 Government Technology. All rights reserved.

**Qwest** is a registered trademark of Qwest Communications International Inc. Other trademarks are the property of their respective companies.

# MANAGED SERVICES

## A How-To Guide

### Table of Contents

<b>Introduction to Managed Services</b> .....	4
What is a managed service?.....	4
Categories of managed services.....	5
How a managed service works.....	5
Reasons for using managed services.....	6
<b>Managed Services 101</b> .....	12
Common managed services.....	12
Integrated managed services.....	15
<b>Acquiring Managed Services and Managing Performance</b> .....	17
How and where to get managed services.....	17
How to define your managed service requirements.....	18
Structuring the service contract.....	21
Managing service performance.....	22
Reporting.....	24
When reports indicate problems.....	25
Meetings with the service provider.....	25
Looking toward the future.....	26

# INTRODUCTION TO MANAGED SERVICES

## WHAT IS A MANAGED SERVICE?

A managed service is a service you purchase from a vendor with the expertise, personnel and infrastructure necessary to deliver exactly what you need, when you need it.

One type of managed service can be thought of like a toll road. The entire road is available anytime you need it, 24 hours a day and seven days a week. You can use it to travel 5 miles or 100. But you don't have to raise the funds to build the road or hire contractors to design and construct it. You don't worry about filling the potholes, plowing the snow or paying the state police to patrol it. You pay a fee to assure the road is available when you need it.



Like toll roads, managed services generally involve large, complex constellations of infrastructure and personnel. In the case of information technology services, they often encompass elaborate hardware and software, with large data centers to house them and staffs of trained personnel to keep them running 24/7.

Like a toll road, a managed service provides excellent value because you share the cost with other users. By serving multiple customers from the same facility, the managed service provider (MSP) offers economies of scale that you could not achieve on your own. You split the cost of using the most advanced technology with other users and gain access to highly experienced IT experts. But you pay for only as much of those resources as you actually need.

While it allows you to share the costs, a good MSP makes you feel like you have the service all to yourself. It's as though you were speeding down the New Jersey Turnpike with no other car in sight. If you buy a managed firewall service, for example, you get 100 percent of the service you paid for. You're not aware that other customers are receiving the same service, maybe even on the same hardware array. You don't see your neighbors, you don't hear them and they don't affect the quality of your service. Nor do they compromise your privacy or security. The service provider sees to it.

## CATEGORIES OF MANAGED SERVICES

Practically any service that an organization prefers not to operate on its own can be outsourced to an MSP. The most popular candidates are complex services, services that involve a great deal of data, those that require expensive equipment and those that require a large staff, or staff with very specific expertise. Some likely areas include:

- Data center operation
- Network management and security
- IT systems maintenance and troubleshooting
- Data storage, including backup and archiving
- Virtual private networks (VPNs)
- Voice networks, including voice over IP (VoIP)
- Converged voice and data networks
- Disaster recovery and business continuity
- Call center technology
- Turnkey call center services
- Managed unified communications

## HOW A MANAGED SERVICE WORKS

The primary parties involved in a managed service are the agency and the MSP. The service provider may work with many subcontractors, and of course, it purchases hardware and software from numerous vendors. It might also provide facilities, such as local telecommunications capacity. But all those relationships are transparent to the agency.

That means the agency doesn't have to worry about evaluating network routers, bargaining for a better price on operating system software or ensuring that data packets transmitted from St. Louis to Los Angeles arrive in good shape every time. The agency benefits from a vast network of product and service partners but receives just one invoice. The MSP handles all the relationships required to ensure the promised level of service.

Within this relationship, the service provider's responsibility is to maintain flawless and seamless performance, delivering service that meets the agency's requirements and expectations as outlined in their contract. The agency's responsibility is to purchase services intelligently, making sure to contract for the kind and quantity of services the organization needs.

The roles and responsibilities that the agency and service provider play may be flexibly negotiated. Essentially you can develop a relationship to provide any combination of services you require. For example, the MSP could:

- Install all the equipment needed to perform the service on the agency's premises.
- Provide a service using equipment in its own facilities, connecting its equipment to the agency's through the service provider's infrastructure.
- Work shoulder-to-shoulder with agency personnel to deliver integrated solutions.
- Provide shared personnel who support common cross-agency initiatives or the needs of multiple agencies.

In many cases, an agency purchasing managed services has its own IT staff — sometimes even a large one — and it might run its own network operations center. Such an organization probably will outsource specific services that management has decided not to operate in-house, such as off-site data storage. Other agencies have little, or no, full-time IT staff. These organizations might turn to a provider for a broad range of IT services, since they're not in a position to run a full-service IT shop on their own.

The key mechanism in a managed service contract is the service-level agreement (SLA). This defines exactly the kind and quality of service the provider will deliver. It might guarantee, for example, that a system will be up and running at least 99.999 percent of the time, or that once a trouble ticket is opened, a technician will arrive to fix the problem within eight hours. Providers charge different rates for different levels of service. An agency that purchases a list of services can choose different service levels for different service components, mixing and matching to tailor the package to its needs.

## REASONS FOR USING MANAGED SERVICES

**They offer a cost-effective way to improve service delivery to an agency's constituents.**

Government agencies are continually under pressure to improve their services to constituents while spending tax dollars wisely. In difficult economic times, those pressures grow even more intense. Managed services provide efficiencies that let governments continue to expand their services while spending less money.

**They allow you to improve existing IT functions without spending a lot of money.**

The IT applications that government agencies use today to perform their missions rely on a complex and expensive technology infrastructure. The most sophisticated applications require the latest servers and the fastest, most reliable networks. These applications deliver

full value only when the underlying technology functions properly and stays up and running around the clock. Agencies also must ensure their IT systems stay safe against attack, to protect the integrity of their operations and safeguard the privacy of the citizens they serve. By taking advantage of a managed service, an organization can continually improve its IT capabilities without having to make continuous investments in new technology and training.

**They eliminate the need for large up-front capital expenditures.** In a tough economy, the capital budget often is the first cost center an agency trims. No matter how badly you need new data storage systems or a network operating center, you simply don't have the money required to build that resource. When you deploy a managed service, however, you gain the use of the infrastructure you require to accomplish your mission, with no need to invest millions at the outset. Instead, you pay a monthly service fee, scaled to your precise needs and drawn from your operating budget.

**They eliminate the need to hire extra staff.** The service provider employs the people required to operate your service. The agency pays only a fraction of the cost of those employees, proportional to the amount of service used.

**They deliver economies of scale.** To run its business and serve its numerous customers, the service provider builds an infrastructure from the most advanced, most reliable technologies available. An agency working alone probably could not afford to buy this level of technology. As an MSP customer, the agency benefits from some of the fastest, most powerful, safest and most reliable IT products on the market without paying full price for their use.

**They offer access to valuable technology and expertise.** If you don't have the budget to keep upgrading your systems to the next level, it's easy to fall behind. MSPs must keep up with the latest technology; without it, they can't stay in business. Not only do they have the money to invest in cutting-edge systems, they also operate research and development laboratories to test new vendor equipment and customize it for use in production. The typical government agency doesn't have the time, staff or



money to stay ahead of the technology curve in all areas. But when that agency contracts for a managed service, it gains a partner that is making those investments continually.

By the same token, an organization that uses managed services benefits from levels of expertise that it could never afford to bring into its own organization. If there's a problem with your wide-area network, for example, you might need a technologist with advanced certification in a specific switching technology to find a solution. That kind of expert commands a large salary. But since problems of that kind don't arise every day,

or even every month, you probably can't justify keeping such an expensive technologist on your staff. An MSP, however, might have several technologists on staff with that specific expertise. When you need them, they stand ready to solve your problem. When you don't, they serve other customers and you don't bear the cost.

**They eliminate the need to buy everything yourself.** As consumers, we're all familiar with the idea of paying for a service rather than buying all the components required to provide that service for ourselves. Say you're on vacation in the Rocky Mountains and you want to go white-water rafting. You could buy a raft, enough paddles for all the people in your party, helmets and wetsuits, and a trailer to transport the equipment to your launch site. But if you don't have a lot of time, and you don't know how to evaluate equipment as you shop, and you're heading home to Atlanta at the end of the week, you probably don't want to make these purchases. So instead, you visit a white-water outfitter and buy a trip package that includes the equipment you need during the hours you spend on the water.

Similarly when you contract for a managed service, you leave it to the service provider to choose, install and operate the hardware and software required to deliver your service. The terms of your contract dictate that you must receive the service. If a problem arises, the service provider is responsible for hunting down the source and providing the necessary fix, whether that means making adjustments or repairs or swapping out a malfunctioning component.



**They eliminate the need to do everything yourself.** Just as a managed service eliminates the need to buy everything internally, it also lets organizations shed the responsibility of doing everything internally. You might be perfectly able to change the oil in your car. But your job and family keep you busy. Your mechanic has a hydraulic lift and other tools that help get the job done much faster than you could in your driveway. It's better to drop the car off before work, spend the day on more productive activities, pay the mechanic and drive home.

The same logic applies to a managed service. It allows you to outsource the work your organization prefers not to handle in-house — because you don't already have the staff, expertise or infrastructure to do a certain job, or because it's more effective to deploy your professionals in other areas. Your organization retains the functions it is best equipped to perform, and your employees can focus on work that provides the greatest value to your agency. Instead of monitoring loads on the network or troubleshooting desktop computers, for example, they might concentrate on developing new strategies for using technology to support the agency's mission.

There are, of course, advantages to keeping certain technology functions in-house. When there's a problem with equipment on your premises, for example, an in-house expert might be able to respond faster to a trouble ticket than one who needs to travel from another location. A well framed contract for managed services, however, will guarantee response times and other service levels that meet your needs.

**They reduce the need to train your staff.** When you outsource particular jobs to an MSP, you also gain the ability to leverage newer technologies without taking your own employees away from their primary responsibilities. Given the work you need to accomplish, it might be difficult to send a member of your staff to attend a weeklong class. An MSP can continuously send members of its staff for training in new technologies, while other employees remain to serve your organization.

**They allow you to focus on your core business.** Many government agencies' primary business is to provide services to citizens. To fulfill that mission, an agency might have developed a large, sophisticated telecommunications organization. But it's not always in the interest of the agency, or its constituents, to let that organization grow and assume more responsibilities indefinitely. A relationship with an MSP lets an agency continue to expand its telecom capacity without necessarily expanding its organization.

**They eliminate the need for you to become an expert at the component level.** If you're having trouble digesting your food and you feel dizzy and nauseous, you'll probably visit

## Trusted Internet Connections (TIC) initiative

On the advice of the Department of Homeland Security, the Office of Management and Budget (OMB) launched the Trusted Internet Connections (TIC) initiative in 2007. This program aims to vastly reduce the number of external Internet connections the federal government maintains. The ultimate goal is to make it easier to defend federal IT systems against cyber-attacks.

Under the TIC, a federal agency can choose to become a TIC access provider or it can purchase Managed Trusted Internet Protocol Services (MTIPS) from one of the major telecommunications companies that have services available under Networx to provide them.

At first, IT officials at many agencies planned to become multiservice providers, or at least to provide Internet services just for their own agencies. But as they explored all the costs and responsibilities involved, many agencies determined they didn't have the experience it takes to serve as an ISP and maintain the necessary infrastructure. Developing that experience and expertise, building the infrastructure and employing people to run the service would just distract agency officials from their core business. Because of these challenges, most federal agencies have decided to purchase Internet services from a Networx provider — an MSP that specializes in this function.

your family doctor to diagnose the problem. If your doctor determines that the trouble lies in your gall bladder, he or she will refer you to a physician who specializes in that organ. If it comes time to remove the gall bladder, the doctor who operates will be not only a surgeon, but also a specialist in gall bladder surgery. Other highly competent surgeons may specialize in problems of the heart, brain or spine, but to correct your problem, you need someone who has spent years studying the gall bladder in particular.

In the same way, many professionals might be able to pinpoint a problem on your network, but if the difficulty lies in the firewall, you need a firewall specialist. Such a person is harder to find and more expensive to employ than an IT generalist. Someone who knows how a particular firewall works in a specific network traffic application is even harder to find and more expensive to employ. And the person who has that expertise and also knows how to program every last aspect of the technology is rarer and costlier still. You probably can't justify keeping such a person on your payroll or training your existing staff to handle all the subtleties of every component in your operation. You don't need that expertise all the time. But when you do need it, you probably can't get by without it. An MSP does employ specialists with the component-level expertise to keep its infrastructure running and serving its customers.

**They can simplify management.** When you rely on an MSP, you don't need to sweat the details. The service provider maintains the staff, forecasts future needs, budgets for equipment upgrades, oversees quality, holds planning sessions, trains employees and handles all the other tasks required to run the service day to day. The MSP also manages the risks involved in running the service, guarding the infrastructure against cyber-attacks, providing backup power and redundant processing capacity and otherwise planning for contingencies that could interrupt your business.

**They allow you to deal with just one vendor.** No matter how many vendors — of hardware, software, network capacity, technical manpower and more — are required to deliver the service, you receive a single invoice. If there's a problem, you don't get caught in the crossfire of finger-pointing wars. Your service provider is responsible for delivering as promised, period.

**They simplify the job of monitoring service quality.** The service provider supplies the tools to help you ensure that services are running as expected. The agency might receive a monthly report with statistics on all the relevant parameters of the managed service: traffic on the network, processor loads on specific machines, cyber-attacks detected and foiled, trouble tickets opened and completed, and a host of others. The reports also would indicate how well the service provider has lived up to its SLAs. As an alternative to



monthly reports, managers at the agency site might log into a portal and access a dashboard, which displays any service data managers need whenever they need it.

Along with helping the agency evaluate the service's past and current performance, the reports and dashboards help with forecasting. Charts that indicate usage, processing loads, power loads and other factors help agencies determine when they will need more capacity; this allows them to budget more accurately for future investments.

# MANAGED SERVICES 101

If you want to start outsourcing some of your agency's functions to an MSP, what's the best place to start? Depending on the size, composition and current activities of your organization, the answer can vary widely. But a few basic principles apply.

You might bring in an MSP when you need a service that:

- **You want to upgrade from a current technology to next-generation capabilities.** A managed service eliminates the need to make large capital investments, hire new staff or acquire knowledge you don't already possess.
- **Requires expertise you don't already own.** It's easier to take advantage of the service provider's existing large, well run infrastructure than to build one yourself.
- **Requires capacity that would be hard for you to obtain.** A health clinic that is outgrowing its ability to store huge medical imaging files, for example, might rely on a managed service for that capacity rather than purchase a room full of storage arrays and hire qualified technicians to maintain it.
- **Requires more attention than your current staff can provide.** If you hire experts to operate a service on your behalf, your employees can focus on the tasks they do best and that provide the greatest value to your organization.

A good way to determine if a service is ripe for outsourcing is to conduct a cost/technology tradeoff analysis:

- **List all the costs required to obtain, operate and maintain the service.** Those costs might include hardware, software licenses, system maintenance, power, heating and cooling, salaries and benefits for employees to run the service, training for those employees, and more.
- **Consider whether your organization has the internal expertise to run the service.** If you need workers with special qualifications, do the needs of the system justify keeping them on staff full time?

If the cumulative cost of obtaining and operating the system is more than your organization can justify, a managed service could be the most effective way to reach your goals.

## COMMON MANAGED SERVICES

**Routers and other IP devices** — Since the mid-1990s, government agencies have been relying on service providers to configure and manage routers and other network devices on their premises.

**On-site maintenance and troubleshooting** — A service provider can take over responsibility for keeping desktop systems, local area networks and other on-premises equipment up and running. This service category includes scheduled installations and maintenance as well as on-call visits to attend to malfunctioning systems.

**Intrusion detection** — Many organizations turn to managed services for network intrusion detection, virus prevention and content monitoring. Large-scale intrusion detection requires round-the-clock attention from highly trained professionals working in a network operations center (NOC), a

large, sophisticated facility that, to a layperson, looks like NASA's Mission Control. These professionals monitor traffic flows and network sensors for unusual activity. They must know how to recognize an adverse event and when they find one, eliminate the problem.

**Virus prevention and content filtering** — To detect spam, viruses, adware and other malicious code, and stop it before it does any harm, you need to keep your software current with the newest security updates. Often, those updates come out several times per day. MSPs have the resources to stay one step ahead of hackers, spammers and other threats at all times. A managed virus prevention and content filtering service can allow authorized personnel at the agency's site to: define filtering preferences; create safe lists for material that always should be allowed to get through; create blacklists for material that should never be allowed to get through; view reports and statistics about messages; and search the database of quarantined material.

**Firewall management and implementation** — To the uninitiated, a firewall appears to be a magic box: you plug it in and it protects your IT systems. But a firewall is an extremely complex system, applying a vast variety of rules to control access by different users and user groups. An administrator must abide by those rules when adding and deleting users and adjusting



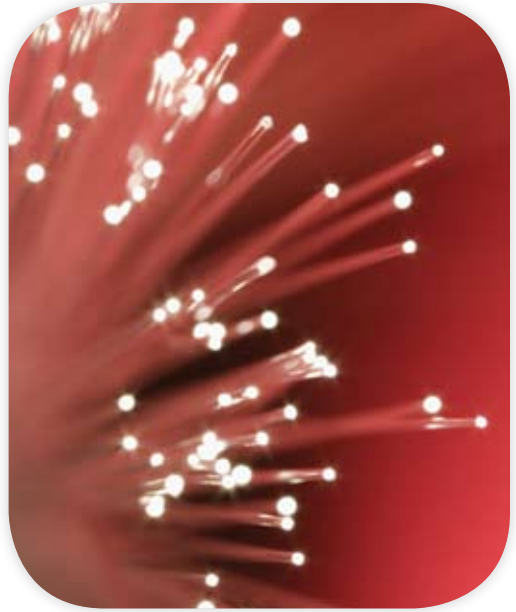
their privileges. A firewall also needs a great deal of care to meet its power and cooling requirements and to back it up with auxiliary power, cooling and telecommunications circuits to keep it operating in an emergency. Instead of letting the MSP manage the agency's firewall, the agency might choose to operate its IT systems entirely within the MSP's firewall.

**Vulnerability testing** — The service provider might periodically scan the agency's network to identify security vulnerabilities. Alternatively it might have engineers run simulated attacks against the agency's network. In either case, the provider uses the results of these tests to make suggestions for correcting weaknesses in the agency's infrastructure.

**Other security assessments** — Besides simulating threats to identify security gaps in the agency's network, the MSP might conduct a technically based analysis of the agency's IT infrastructure and then develop suggestions for improvements. The provider also can analyze an agency's business policies and processes to make sure they foster a secure IT environment.

**Hosting environment** — Rather than run applications on servers it maintains on its own premises, an agency might have them reside in a hosting center operated by an MSP. The service provider is responsible for keeping the servers up and running, providing the necessary environmental controls and managing the server hardware and software, including operating system upgrades and patches.

**Storage area networking and data warehousing** — Agencies that produce large volumes of data need elaborate storage facilities to manage backups and meet data archiving requirements. The necessary storage arrays can be cost-prohibitive, especially for organizations whose core business is not managing data, but serving constituents. In the world of physical goods, rather than get into the warehouse business itself, a company



with large volumes of product to store might lease space in a public warehouse. In a similar way, an agency that needs to store and protect large volumes of data, but that doesn't want to get into the data storage business, can rely on the vast capacity available through an MSP.

**Disaster recovery and business continuity** — Off-site backup systems and rollover facilities let agencies continue serving constituents when power failures, natural disasters and other disruptions make it impossible to use their primary IT facilities.

## INTEGRATED MANAGED SERVICES

Once an agency has turned to a provider for one or more large, IT-intensive services, officials may find the arrangement so beneficial they want to tap the provider's capabilities in other ways as well. Services that an agency might outsource at a later stage include:

**Virtual private networks, including virtual WAN and Ethernet** — AVPN allows remote users to interact with a central IT system over a public network, usually the Internet, while enjoying the functionality and security of a private communications link. VPNs are created by means of hardware devices called VPN concentrators, which limit access to specific IP addresses and specific numbers of participants. It takes a high degree of expertise to configure and maintain these devices and administer their use.

**Voice communications** — Even in a world that has embraced digital communications, many offices, especially smaller ones, still use legacy analog telephone systems. Rather than keep someone on staff with the knowledge to maintain their private branch exchange (PBX) systems, many of these organizations contract with vendors to keep their voice systems operating correctly.

**Voice over IP** — In a VoIP system, many functions that used to occur within the PBX hardware on the user's premises now occur in software. The transition to digital voice communications also enables many new functions that weren't possible under analog, such as the ability to access voicemail messages over the Internet. The software-based intelligence that drives a VoIP system doesn't need to reside within the agency's four walls. A service provider can operate the VoIP system in a hosting center, just as it would any other server-based application.

**Converged voice and data** — A digital network doesn't care whether the packets it moves ultimately represent a series of spoken words, a record in a database or a pie chart. As agencies migrate to digital VoIP services, the opportunity arises to manage those services

on the same platform as other data functions. Technology available today makes it possible to manage mixed traffic effectively on a network, making sure, for example, that voice and video — whose quality depends on reliable delivery — take precedence over generic data transmissions. Managing voice and data on the same communications infrastructure allows an organization to enjoy yet another economy of scale. Instead of employing separate groups of experts to manage the data and voice operations, it can use the same staff to take care of both. When an MSP delivers these converged services, it can pass the economies of scale along to its agencies.

**Contact centers** — An MSP, especially one run by a major telecommunications carrier — can provide call center services at any level the agency needs. At the lower end, it can provide just the toll-free calling service that constituents use to call service representatives. It can provide interactive voice response (IVR) technology, which uses menu trees to obtain information from the caller about the question or problem that spurred the call. It also can provide an automatic call distribution (ACD) system, which uses data entered through the IVR to route the call to the appropriate system or agent. At the higher end of the scale, the carrier can provide agents to staff the call center. Alternatively it can provide a turnkey call center service. Under that model, the carrier employs the staff and operates the center in its own facilities, handling calls from constituents according to the agency's needs and specifications.

**Cloud computing** — With the growing popularity of software as a service (SaaS) — or computing in the “cloud” — hosted applications have a great deal of potential as managed services. Just as MSPs now own and operate servers to host their clients' applications, and arrays to store the data those applications generate, they also can own and operate the applications themselves, delivering as much or as little functionality as agencies need. And just as the service arrangement frees the agency from having to maintain server operating systems, a managed cloud computing environment makes the service provider responsible for upgrading applications as new versions become available.

**Integrated management** — By bundling several services into an integrated package, a service provider can take over the burden of running and safeguarding a major portion of an agency's IT operation. This is particularly helpful for organizations that don't have sophisticated internal IT capabilities.

# ACQUIRING MANAGED SERVICES AND MANAGING PERFORMANCE

## HOW AND WHERE TO GET MANAGED SERVICES

The managed service landscape is evolving. Many agencies today turn to telecommunication companies as a natural choice for such services as network security and next-generation “as a service” offerings.

Agencies can contract for managed IT services under several federal contracts.

**Networkx** is the largest contract federal agencies use to obtain services from telecommunications companies. Overseen by the General Services Administration (GSA), Networkx is composed of two broad vehicles:

**Networkx Universal**, awarded in March 2007 to Qwest Government Services, AT&T Corp. and Verizon Business. This contract provides comprehensive telecommunications services worldwide, covering a range of services in six categories: telecommunications, IP-based, optical, wireless, management and application and security. Of those services, 36 are offered by all of the contractors.

**Networkx Enterprise**, awarded in May 2007 to Qwest Government Services, AT&T Corp., Verizon Business Services, Level 3 Communications and Sprint Nextel Corp. The contract covers emerging IP and wireless services nationally in the same six categories as Universal. It includes nine that are offered by all of the contractors.

More detail on Networkx is available at: [www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA\\_OVERVIEW&contentId=16100](http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16100)

Essentially any sort of managed telecommunications service an agency could want is available through Networkx. Under this contract, vendors also can perform customized engineering, perform other design work and locate staff on an agency's premises to run network operations centers, for example.

Networkx is a competitive contract. An agency that uses this vehicle to obtain a managed service would compete their requirements among the Networkx vendors to determine who offers the best value.



**GSA's Information Technology Schedule 70** allows federal government agencies to procure a wide variety of IT products, services and solutions. Schedule 70 lists a large number of vendors that can meet the needs of agencies in the following areas:

- Leasing of products
- Daily/short-term rental
- Purchase of equipment
- Equipment maintenance
- Term software license
- Perpetual software license
- Software maintenance
- Classroom training
- Information technology services
- Electronic commerce services
- Wireless services
- Authentication products and services
- Public key infrastructure (PKI) shared services provider (SSP) program
- Homeland Security Presidential Directive 12 product and service components

More information on GSA's Schedule 70 is available at [www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA\\_OVERVIEW&contentId=8661](http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=8661)

**Governmentwide Acquisition Contracts (GWACs)** are task order or delivery order contracts that one agency has established, but that can be used throughout the government. Agencies may use these to purchase managed services. More detail on GWACs is available at [www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA\\_OVERVIEW&contentId=16146](http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_OVERVIEW&contentId=16146).



## HOW TO DEFINE YOUR MANAGED SERVICE REQUIREMENTS

**Define your needs.** The first step in framing the requirements for a managed service is to thoroughly outline what you want the service to do for you. List all the functions you need the service to perform, the results you are looking to achieve, the management process you wish to simplify and the standards of service you require.

**Inventory your current service.** If the managed service will replace one you now operate internally, you will need to understand every aspect of the service as it exists today. This understanding helps ensure the managed service will continue to meet the

needs of your agency's user community. If the switch to a managed service eliminates certain functions that users expect to have available or provides lower service levels than users are accustomed to, they will be unhappy with the new service, even if it offers many new advantages.

**Inventory your current infrastructure**, including hardware, software, network topology and licenses.

**Include all stakeholders in the process.** This helps ensure that as you develop your requirements, you consider the perspective of everyone in the organization who has an interest in the service. You probably will want to include members of executive management, technology management, network staff and the accounting department. If the service provider will place any of its own employees on your premises, you may need to involve the human resources department.

**Don't forget end-users.** The stakeholder committee that helps to inventory your current service and define your needs should always include representatives of the people whose jobs will be affected by the outsourced service. End-users can provide invaluable insight into your current service. They can tell you which features are essential to getting their work done, the improvements they would like to see, the service standards they consider essential and the kinds of changes they would find disruptive.

**Be honest and accurate about your requirements.** Make sure you understand the difference between "must-have" and "nice-to-have" features.

**Define your budget and prepare your business case.** Understand how much you're willing to spend and how much extra you can afford for nonstandard services that require negotiation.

**If you need help determining your requirements**, issue a request for information (RFI) to solicit advice from the community of MSPs. You may also want to hold an industry day to glean insight from the MSPs in the industry. Attending industry tradeshow will also give you a broad array of what is available and possible for managed services.

**Research the market.** Make sure you understand the vendors' standard offerings. The federal contracts described above list in detail the services that vendors are ready to provide. The basic unit of a service offering is the SLA, which defines exactly what the provider will deliver and to what standard. In the Networx contract, the GSA mandates that vendors providing specific services deliver a specific set of SLAs for each one. In some cases, vendors state that they will exceed those SLAs. If the SLAs as defined in the contract

meet your needs, you are well on your way to understanding what a given provider will offer in a managed services environment.

**Consider conducting service pilots** to clearly identify core and support services and dependencies.

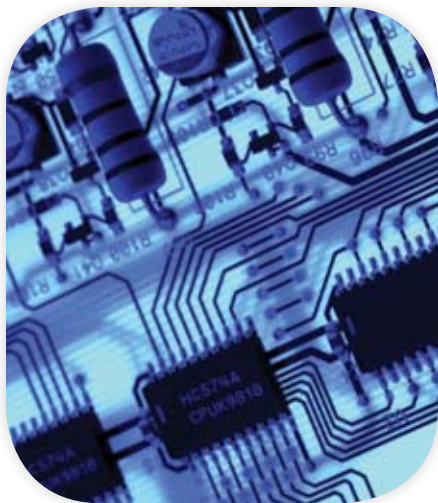
**Identify requirements that aren't part of the standard offering.** Your agency might have special needs that exceed some of the SLAs defined in a vendor's offering. For example, a vendor proposing to manage a VoIP service over your wide-area network (WAN) needs to offer a latency guarantee, to make sure real-time voice packets arrive in a timely manner.

You should ensure this guarantee matches the level of voice quality you require. You may also want an SLA governing jitter, which is the variation in the time it takes to transmit digital voice packets. If the vendor's offering doesn't include an SLA to cover jitter, you can ask for one.

**Be prepared to make tradeoffs.** It might not be possible for the service provider to deliver the SLA you want while using the technology architecture you specified. Say, for example, you want to run low-speed telecommunications circuits to remote offices. The carrier might be able to promise only 99.99 percent availability on that kind of circuit. If you really require 99.999 percent, the carrier might propose an alternative network architecture. This probably will cost more. When this dilemma arises, ask yourself, "Do we really need that extra level of availability? If so, what are we willing to pay for it?"

**Find out not just what vendors will deliver, but how they will deliver it.** For example, if you require end-to-end reporting on your service, ask service providers to explain how they plan to meet that need, including specific deliverables and time frames. If the reports included in their standard offering don't meet your needs, you can negotiate for a reporting package tailored to your requirements.

**Develop credible, logical evaluation criteria, and document them.** In federal procurements, unsuccessful bidders often protest contract awards. To make sure you award the contract to the bidder that genuinely meets your needs, it's important to demonstrate that your RFP and your evaluation criteria comply with federal acquisition regulations.



**Don't make your decision based entirely on price.** The cheapest solution may not be the best, and the most expensive solution might deliver more value for the money than a moderately priced one. Carefully examine all the cost/technology tradeoffs to determine which proposal offers the best value at a price you consider acceptable.

**Select a service provider you trust.** If you have obtained other services from a particular provider and were happy with the relationship, that company is a good candidate to provide your new service.

**Obtain corporate qualifications and references that address past performance.** Firms with a reputation for high-quality delivery, excellent customer service and ample technical breadth are good candidates for managed services.

**Ask for documentation.** When a service provider claims a particular level of experience or capability, can it back up that claim? For example, if you are procuring security services, you probably will want to see a Statement on Auditing Standard 70 (SAS70), which documents the fact that the service organization has passed a vigorous audit of its internal controls.

## STRUCTURING THE SERVICE CONTRACT

The managed services contract defines the relationship between the service provider and the client. It outlines all the services the provider will deliver, with an SLA to define precisely what each of those services will consist of. It also defines the provider's liability if it does not deliver on each SLA.

The contract should include a performance work statement (PWS) and a quality assurance plan for assessing performance. Essential components of the contract include both business and technology performance requirements as well as performance standards and measurements for meeting your business needs. It also should outline any allowable deviations from the performance standards — the acceptable quality level.

Include options for support such as consultation, design, engineering and implementation to provide for change in the networking environment.

Provide a notification process for infrastructure changes or planned outages.

The GSA does a good job of establishing a baseline for its managed service contract, including many predefined SLAs for each type of service and for the management components to be applied on top of the service. If you have SLA requirements that supersede any of the baselines, make sure to include those in your statement of work.

Payment terms for a managed service contract often involve a flat monthly fee over the lifetime of the contract. The fee is based on the services provided, the particular SLAs covered and the number of desktops or other devices the service covers. It is also possible to structure a contract with different payment terms, depending on the nature of the service. For a maintenance and troubleshooting service, for example, an organization might purchase a block of service hours and add more as needed. Some contracts might be based on usage volume.

### MANAGING SERVICE PERFORMANCE

#### Service-level agreements

Just as the SLA defines the service a provider will deliver under a contract, it provides a standard for measuring service performance. We enter into SLAs all the time. If you subscribe to a local newspaper, for example, your agreement with the publisher may stipulate that a paper will arrive on your doorstep by 7 a.m., seven days a week. If you open your door at 8 a.m. on Saturday and don't find a paper, the publisher has violated your SLA, and you can seek redress.

In a managed services agreement, the SLA is a guarantee. If the provider contracts to keep your network running 99.999 percent of the time, but you find that in a given week the uptime is only 99.99 percent, the provider has violated the agreement. If the contract

#### Exceeding the baseline

Managed service providers that are included in the General Services Administration's Networkx contracts may offer SLAs in their standard agreements that exceed the GSA's baseline SLAs. A case in point is multi-protocol label switching (MPLS), a next-generation, IP-based WAN technology available as a service under Networkx. GSA's baseline SLAs for MPLS do not include an agreement to address jitter, the variation in the flow of data across a network. But many federal agencies are likely to use MPLS to deploy voice and video applications, making jitter a crucial factor. Too much variation in packet delivery creates problems for voice and video, including popping sounds, pauses and frozen video frames. An MSP that understands the importance of voice and video services could choose to exceed the GSA's baseline requirements and include a jitter SLA in its standard offering for MPLS service.

Some providers include quality of service (QoS) as part of their basic MPLS service offering. Other providers charge for the addition of QoS. A careful comparison of your actual requirements and the prices for services offered will help determine the best value.

states that a technician will arrive to fix a problem at your site within eight hours of a trouble call, and one day a technician takes nine hours to arrive, that's a violation as well.

Because the contract for managed services may include financial penalties, it is in the interest of the service provider to stand by its SLAs. The managed services contract includes an agreement on how the provider and agency will measure successful performance, who will do the measuring and what data the agency will receive to document performance.

In broad terms, an SLA:

- Describes what the service provider will do.
- Defines a performance target, such as 99.999 percent availability.
- Describes how the provider and agency will measure performance against that target.
- Specifies a penalty for missing that target, and in some cases, a reward for exceeding it.

The SLA probably will include different provisions for different situations. For example, the Networx contract specifies a shorter mean time to repair for problems the service provider can fix remotely than for problems that require a site visit. For on-site repairs, a typical mean time to repair is eight hours. But if some of the agency's sites are in remote locations — say, rural Alaska — the SLA might specify that the mean time to repair for those sites is the next business day.

The following are some best practices for ensuring that the SLAs in your contract support your organization's goals:

**Read each service agreement in the proposed contract carefully.** Maintain a critical eye for the details.

**Get help from your procurement organization.** You might understand all the technical aspects of the contract, but it helps to have a second critical reader, especially one who knows how to spot loopholes and is attuned to questions of responsibility and liability. All agencies have a contracting officer that can assist with this process.

**Make sure you understand the definition of each key term in the SLA.** For example, do you and the service provider agree on the definition of "availability"? Be sure to eliminate any ambiguities, and be sure each term is used in the same sense throughout the agreement.

**Double-check the metrics.** Make sure you and the provider agree on how performance will be measured and reported, so there is no cause for dispute once the service begins.

**Define responsibilities.** If the picture on your TV is fuzzy because of a problem at the utility pole, your cable TV company will fix that problem. If the picture is fuzzy because your

20-year-old set is getting ready to die, you'll need to buy a new TV. The same applies when you're working with an MSP. If your network is slow, it might be the MSP's fault, but it might also be the fault of your internal technology. Make sure you understand the difference.

**Nail down all the details before you sign.** Don't leave any loose ends or ambiguities to work out after the contract goes into effect.

## REPORTING

As we have already seen, the service provider delivers reports — either periodically, or on demand through the Web — to give the agency details on service activity and document the quality of the service.

For example, a contract for telecommunications services might include an SLA which stipulates that latency between any two sites on the network will be no more than 70 milliseconds. A function within the network periodically

polls each end-user site to measure the actual round-trip latency. If the agency receives a monthly report and statistics indicate that average latency during the period was 58 milliseconds, the agency knows the service provider has fulfilled this SLA.

The same holds for a agency who receives reports through a Web-based dashboard. If the graph that portrays network latency shows that, in real-time operation, average latency across the network is 58 milliseconds, this also proves the provider is meeting the terms of the SLA.

Which personnel use these reports depends on the size of the agency and the roles played by various members of the IT team. Typically at least one member of the telecommunications staff will have the job of managing the relationship with the provider. That person would monitor the reports to make sure the provider is meeting the SLAs. Someone in an oversight position, perhaps as high on the organizational chart as the chief technology officer (CTO) or chief information officer (CIO), might monitor service performance as well.



If reports indicate that the service provider has missed one or more SLAs, that information will trigger a discussion. Depending on the terms of the contract and the severity of the violation, it may also trigger a financial penalty.

As you examine SLA reports, be sure to compare them to your actual experience with the service. If the report indicates 100 percent compliance, but you and your team have experienced problems with the service, make sure to discuss the discrepancy with the service provider.

## WHEN REPORTS INDICATE PROBLEMS

Of course, some interruptions in service are inevitable. For example, if a temporary condition on the network forces the agency's traffic to take a different route, that might push latency over the 70 millisecond threshold. Because it is the service provider's business to know about and fix network issues, an alarm mechanism tied to the SLA will automatically open a trouble ticket if it appears to constitute a trend. A service technician in the NOC will then examine and fix the problem. When the agency views a report for this period, the latency graph will show a sudden spike and then a return to normal, indicating the problem has been fixed.

Not all reporting can wait until the end of the month or until the agency logs in to access a performance dashboard. An SLA might stipulate that if there's a particularly grave problem — say, a serious attack on the network — the provider will contact the agency within a defined period, perhaps two or four hours. If the problem is extremely serious, the agreement might stipulate that the agency will get word in as little as 30 minutes. In this case, someone in the agency's organization would carry a pager or cell phone for immediate notification.

## MEETINGS WITH THE SERVICE PROVIDER

At the start of a managed service relationship, the agency and provider probably will want to hold a monthly assessment meeting to review the service reports. If statistics indicate any outages or if certain trends indicate that the provider might miss an SLA in the future, they can use those meetings to discuss those problems. The service provider will identify the source and lay out an action plan, with milestones, to make sure such issues don't recur.

These meetings also provide an occasion to discuss any service problems that are not reflected in the report. It is important to bring these up as soon as possible, so the service

provider can resolve them. Agencies might also bring up questions about their billing or about how to use the report dashboards. In addition, agencies and carriers use these meetings to discuss the status of additional services the provider is rolling out — for example, if it is adding service to a series of local offices.

## LOOKING TOWARD THE FUTURE

As the provider and agency work together over time, they will start to develop a stronger level of trust. At that point, instead of meeting monthly, they might decide to get together every quarter. Once the agency feels wholly comfortable with the relationship, the parties might settle into a pattern of twice-yearly meetings.

Besides providing an opportunity to touch base and discuss any questions the agency has, those semiannual meetings give the two parties a chance to conduct engineering reviews, to ensure the service still meets the agency's needs. Since the service provider can see how heavily the service is taxing various elements of the infrastructure, its employees are in a perfect position to discover when the agency needs more capacity or could benefit from modifying the service. If, for example, a high volume of traffic is straining a particular communications circuit, the provider might suggest upgrading that circuit or shifting some traffic to another one if possible.



These meetings also provide a chance to discuss whether the time has come for the agency to entrust other services to an MSP.

Of course, anyone who uses an MSP should remain vigilant, continuing to monitor service reports to make sure the provider is meeting SLAs. But if you enter the relationship with a clear understanding of your needs and you design an agreement that clearly spells out your expectations, your requirements to supervise will be minimal. The provider will see to the operation of your service, and your agency will be able to focus on its core mission.

## Acronyms Used in This Report

ACD –	Automatic Call Distribution	PKI –	Public Key Infrastructure
CIO –	Chief Information Officer	PWS –	Performance Work Statement
CTO –	Chief Technology Officer	RFI –	Request for Information
GSA –	General Services Administration	SaaS –	Software as a Service
GWACs –	Governmentwide Acquisition Contracts	SAS70 –	Statement on Auditing Standard 70
ISP –	Internet Service Provider	SLA –	Service-Level Agreement
IVR –	Interactive Voice Response	SOO –	Statement of Objectives
MPLS –	Multi-Protocol Label Switching	SSP –	Shared Services Provider
MSP –	Managed Service Provider	TIC –	Trusted Internet Connection
NOC –	Network Operations Center	VoIP –	Voice over IP
OMB –	Office of Management and Budget	VPN –	Virtual Private Network
PBX –	Private Branch Exchange	WAN –	Wide-Area Network

For additional copies or to download this  
How-To Guide, please visit:  
[www.govtech.com/managedservices](http://www.govtech.com/managedservices)

Get Qwest. Get Nimble.™

