A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

Using Managed Services to Overcome Modernization Hurdles

A new generation of services offers expanded capabilities and more control.

Introduction

Staff shortages, skills gaps and increasingly complex network infrastructure are prompting government IT leaders to take a serious look at managed services. At the same time, managed services are evolving to give agencies new options for maintaining control of mission-critical capabilities while addressing talent and technology challenges.

This combination of greater needs and more flexible service models is driving more interest in alternative ways to acquire the necessary skills and technologies for digital transformation.

“There’s a reckoning to modernize, streamline and normalize IT operations,” says Center for Digital Government (CDG) Senior Fellow Sean McSpaden, former deputy CIO for the state of Oregon. “Managed service providers can really be a force multiplier for government organizations.”

Pressing Priorities

Aging technologies, lack of IT staff and inadequate IT skills are at the core of many challenges facing state and local governments. A new generation of managed services may help CIOs impact multiple issues at the top of their priority lists.

State CIO Priorities[1]

1. Strengthen cybersecurity
2. Improve constituent experience
3. Hire and retain competent IT personnel
4. Modernize legacy technologies
5. Expand broadband connectivity

City CIO Priorities[2]

1. Strengthen cybersecurity
2. Hire and retain competent IT personnel
3. Improve constituent experience
4. Expand business intelligence/analytics
5. Improve data governance

County CIO Priorities[3]

1. Strengthen cybersecurity
2. Improve constituent experience
3. Hire and retain competent IT personnel
4. Expand broadband connectivity
5. Upgrade disaster recovery

The Evolution Of Managed Services

Although cloud-based applications and operating models have proliferated in the public sector, many organizations still need to run, maintain, secure and upgrade physical network infrastructure. For state and local governments, that can mean anything from managing in-house data centers and connectivity within a single office or agency to deploying wide-area networks (WANs) to connect offices across a region or state.

Technology leaders face considerable challenges in modernizing and securing this mission-critical infrastructure. As networking technology becomes more complex, skills gaps within IT departments continue to grow. The pandemic also highlighted "key person risk" — when the one person with knowledge of a system or process departs or is unavailable when the technology fails.

Aging in-house network technology also creates barriers to supporting hybrid work for public employees and expanding cloud-based digital services for constituents. These and other modernization needs require network capacity to scale, which can be difficult with old hardware and traditional approaches.

"There's lots of talk about digital transformation of government services, but you can't do that when your whole focus is managing systems that are 20 to 40 years old," McSpaden says. "We have a serious lack of knowledge of the systems and tools available today. We have to move away from legacy thinking."

Managed service providers (MSPs) can help address these challenges in multiple ways. They simplify IT modernization by upgrading network infrastructure and managing ongoing hardware and licensing upgrades over the duration of a contract. They can augment in-house skillsets with additional expertise in areas such as cybersecurity. And at their most expansive, managed service agreements can integrate a broad range of connected devices — including phones, networked cameras and sensors — with the underlying network infrastructure.

MSPs can also help standardize operations and provide a single point of contact for multiple systems, according to CDG Senior Fellow Craig Orgeron, former CIO for the state of Mississippi. Agreements with MSPs have evolved along with technology. Instead of one-size-fits-all models, many providers offer co-management options that let agencies maintain or share control over mission-critical capabilities. And as governments grow more familiar with as-a-service models of modern cloud applications, they are also in a better position to procure managed services.

Managed service providers can simplify IT modernization by upgrading network infrastructure and handling ongoing technology upgrades.

Managed Services by the Numbers

60%

of regional and local governments plan to realign budgets and job categories by 2024 to increase investments in cloud and managed services.[4]

63%

of state technology leaders plan to shift functional areas to managed services to address skills gaps.[5]

67%

of city and county governments use or are considering managed IT services.[6]

The Managed Service Life Cycle

Developing a Strategy

- ☑ Inventory current systems and data
- ☑ Create a vision that reflects your core priorities

Deciding What to Outsource

- ☑ Understand existing capabilities
- ☑ Project future requirements
- ☑ Analyze total cost of ownership

Selecting an MSP

- ☑ Look for a successful track record with government clients
- ☑ Demand an experienced project team
- ☑ Seek flexibility and accountability

Designing a Managed IT Environment

- ☑ Communicate your long-term goals and regulatory requirements
- ☑ Develop appropriate SLAs
- ☑ Specify the scope of co-management

Implementing the Service

- ☑ Ensure existing systems keep functioning during the transition
- ☑ Demand adequate MSP support during the shift
- ☑ Have a fallback plan

Managing the Contract

- ☑ Define staff and MSP responsibilities
- ☑ Monitor service performance
- ☑ Continuously evaluate your MSP partnership

Steps For Success

Adopting managed services often involves some soul-searching for IT leaders and their teams.

“We have to be open to objectively assessing if we’re managing a system where there’s no competitive advantage to manage. We have to be willing to let someone else do it,” McSpaden says. “Sometimes we can’t see the forest for the trees when we’re putting out operational fires every day.”

You’ll need to consider a range of factors to determine where and how managed services fit within your organization.

☑ Developing a Strategy

The first step is understanding your existing IT environment. Begin with a detailed inventory of systems and data. Make sure you understand which systems and data must comply with special security requirements.

From there, develop your strategy for evaluating, implementing and monitoring managed services. That vision must reflect your core priorities, such as expanding constituent service offerings and addressing workforce needs.

“It’s so important to have this vision in mind, but it’s a tough thing to do,” says Orgeron.

☑ Deciding What to Outsource

Next comes deciding which specific systems or capacities should be shifted to managed services. Consider these factors as you decide:

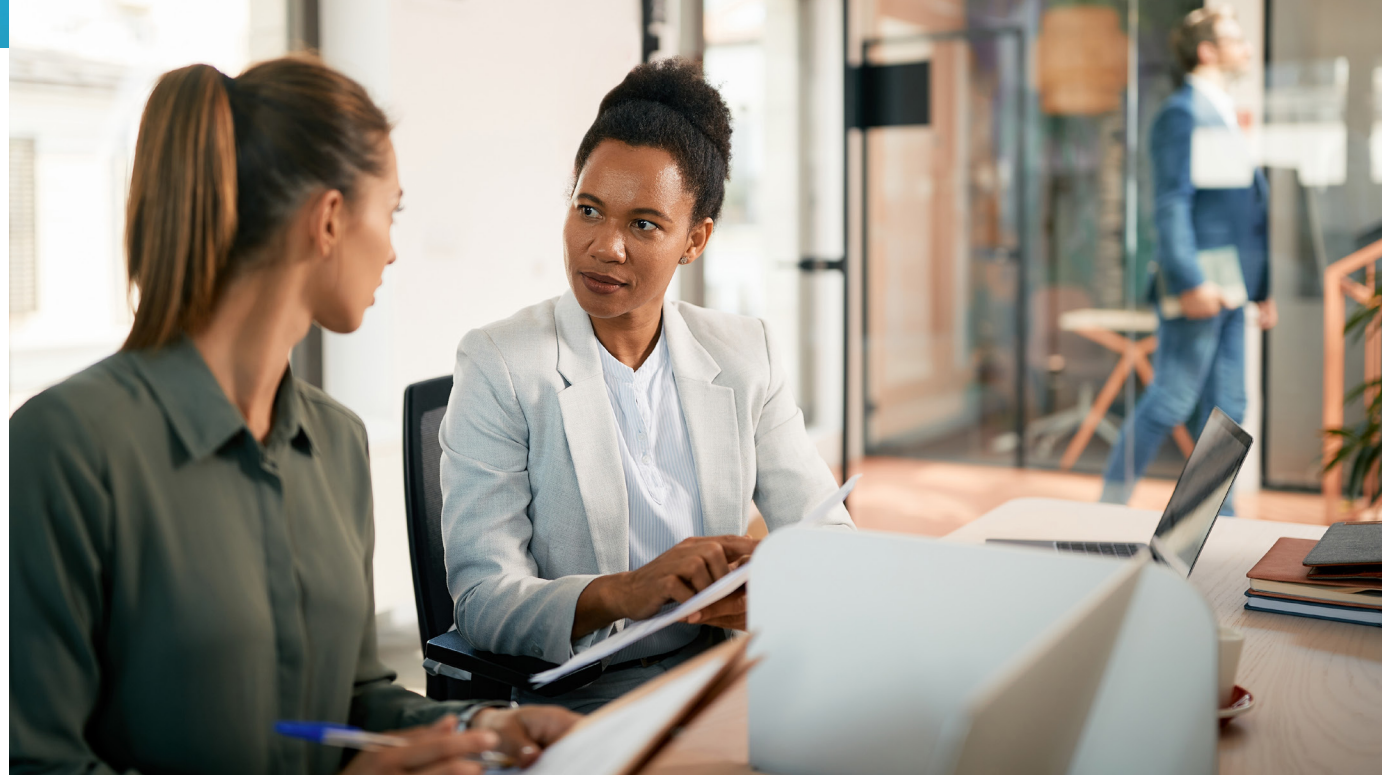
Capabilities of existing infrastructure and staff. Along with understanding current skills and technology gaps, think about your staff’s ability to oversee partners in a managed services agreement. “What happens over time is that these services grow, and they can outstrip the capacity of your organization to manage them,” Orgeron says.

Evolving requirements. Think about your future needs. For example, how will growth of digital services and hybrid work impact your connectivity needs over the next five years? Can your existing networks support these requirements effectively?

“No particular architecture or tool is a silver bullet, and you can get into analysis paralysis about what you need,” says Orgeron. “But you do need the

business plan saying what problems you want to solve and put some thought into using the right tools for your organization."

Total cost of ownership. It's particularly important to understand the full costs of maintaining and modernizing your existing infrastructure — including ongoing maintenance, upgrades and support services provided by vendors — as you examine the business case for managed services. External consultants may be helpful in completing a full cost-benefit analysis, McSpaden says.



☑ Selecting an MSP

Evaluate different MSPs to find the best fit. Consider these factors:

Track record with government clients and projects like yours. If you're modernizing a statewide WAN, for example, look for an MSP with experience in that area. "A desktop environment in a single agency is very different from seat management for 40,000 employees," says McSpaden. "You need an MSP with that demonstrated experience."

Quality and experience of the project team. Understand the capabilities of the project team assigned to you by the MSP. "You need a solid team with depth of knowledge working on similar projects with similar scope and scale," McSpaden says.

Ability to provide support. Government operations often run 24/7, so support capacity is crucial. Does the MSP have significant support teams within your region? Does it promise 24/7 response for critical services? Can the MSP, as one expert put it, arrive with "ladders and bucket trucks" in an emergency?

Critical government operations must run 24 hours a day. Choose a service provider with support teams and resources in your region.

Willingness to commit to service-level agreements (SLAs). MSPs often provide SLA templates. They should also provide sample performance metrics and explain how they'll be held accountable if metrics are not met. "MSPs have to be willing to listen and negotiate," McSpaden says. "Your vendor should have confidence in their services and be willing to be accountable."

Ability to expand government capacity. The right MSP can help your agency adopt innovative technologies at scale. "The more mature their ecosystems are, the more it brings remedy to all the barriers we're talking about, including a lack of automation," Orgeron says.

Flexibility. Unlike vendors selling off-the-shelf solutions, MSPs should be willing to deploy and manage systems tailored to your specific needs.

Ability to avoid vendor lock-in. MSP contracts should include provisions that let agencies shift to another provider or bring operations back in house if the arrangement doesn't work out. "When you are developing and finalizing your contract, don't just think about the marriage.

Think about the divorce, and how you and your MSP will have to work together to get through that difficult process," McSpaden says.

☑ Designing a Managed IT Environment

Communication during the design phase is critical to reduce change orders, avoid extra costs and prevent implementation delays. Here are key steps to take:

Communicate your priorities and goals. Start with the end in mind — make sure the MSP understands your long-term needs and direction. This helps your MSP determine how to design the supporting infrastructure.

Provide documentation. Legacy government systems that have evolved over years or even decades are often poorly documented, McSpaden says. Conducing an inventory of existing systems and data requirements at the beginning of a managed services initiative gives you a head start, but it's vital to give your MSP network diagrams and other documentation to guide design. You'll also need to share information about key stakeholders — such as who uses what systems and data — how systems are used, and how information must be secured.

Adequate vendor support is critical as you move from legacy to modern infrastructure. Your service provider should provide on-site resources to support your transition.

Communicate government-specific security requirements and regulations. MSPs need to know what systems need specialized data safeguards to ensure compliance with federal guidelines and regulations. Document your security requirements for systems and processes, including the use of continuous monitoring required by FedRAMP and StateRAMP. "If you don't document them, those things will come back to haunt you," Orgeron says.

Determine what systems stay and go. Work with your MSP to identify which existing systems will be integrated with the managed environment and which ones will be phased out.

Ensure priorities are reflected in SLAs. Specify key factors, including uptime requirements for mission-critical systems, repair and restoration timeframes, and other support considerations.

Specify the scope of co-management. Co-management can take many forms. Clearly defining roles and functions for your agency and the MSP is a key to success. Make sure both sides understand issues like how help-desk tickets will be handled and the capacity of the MSP to roll back changes made by agency staff.

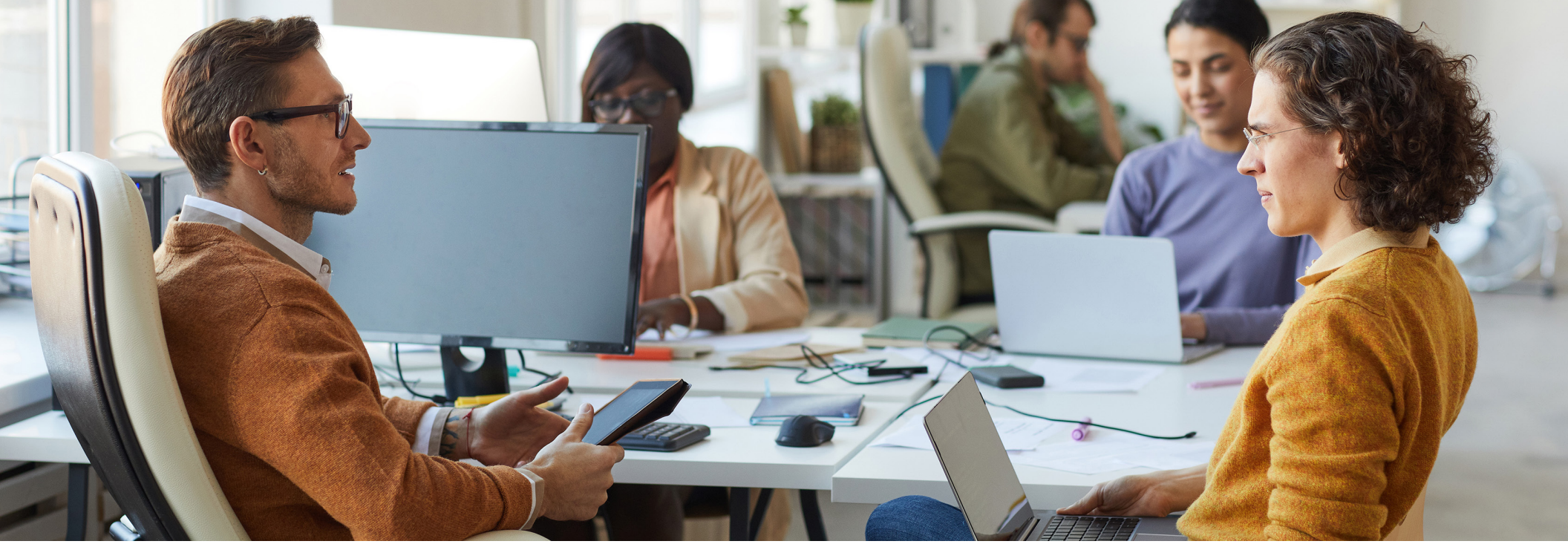
"The worst thing possible is to leave the discussion of roles and responsibilities until the end of the process," McSpaden says. "It comes down to the focus on the SLA, the vendor's willingness to listen, and the willingness of both parties to pick up the slack once they understand what the other can provide."

Determine how much training your staff will need. In many cases, in-house IT staff must transition from operational roles to managerial functions like overseeing contracts and brokering services. "We're all in a place where expectations are changing," says McSpaden. "In many cases, we will need our internal staff to shed the more operational, box-and-wire activities."

☑ Implementing the Service

Careful selection of partners and frequent communication during the design phase should lead to smooth implementation. Even so, "with every transition, everyone understands there will be some bumps in the road," McSpaden says. Here are some strategies for a successful managed services implementation:

Develop transition and fallback plans. Existing systems must continue to function and be



supported during implementation. You'll also need the option to roll back the launch if the new systems don't perform as desired.

Ensure adequate support as systems shift from legacy to modern infrastructure. Your MSP should provide on-site resources to support the transition. "The support team shows its mettle during this phase," McSpaden says.

Upskill staff to support new roles. Use the retraining needs identified in the design phase as a guide. Focus on project management and other higher-level skills.

☑ Ongoing Management

Delineate ongoing staff and MSP responsibilities. McSpaden recommends developing a statement of work for agency staff that outlines the specific issues they can ask the MSP to address. This helps prevent your organization from going beyond the scope of the managed services agreement.

Focus on visibility and continuous monitoring. Understand your options to monitor managed services to identify and troubleshoot potential problems. "If I can't see a managed service beyond the boundaries of my organization, I don't have visibility into what could be the problem," Orgeron says.

Continuous monitoring becomes even more important when securing managed environments that facilitate access to the cloud. "You're probably going to be expanding your perimeter and making it more malleable," he says, "so you have to be thoughtful about that."

Continually evaluate your MSP partnership — and focus on the future. Along with monitoring MSP performance as specified in the SLAs, it's important for IT leaders to focus strategically on future improvements. "Think about how you grow, how you scale, how you offer more services," Orgeron says.

That growth-minded approach is particularly valuable for agencies that adopt managed services to improve constituent services. "The use of managed services is an open door you can take advantage of," Orgeron says. "What typically happens is you gain efficiencies, but there is a larger suite of new and more robust services to pivot and expand your portfolio."

This piece was written and produced by the Government Technology Content Studio, with information and input from Spectrum Enterprise.

Endnotes
1. https://www.govtech.com/cdg/digital-states/digital-states-survey-2022-results-announced
2. https://www.govtech.com/dc/digital-cities/digital-cities-survey-2022-winners-announced
3. https://www.govtech.com/dc/digital-counties/digital-counties-survey-2022-winners-announced
4. https://blog.workday.com/en-us/2023/future-state-local-government-5-essential-focus-areas.html
5. https://www.nascio.org/wp-content/uploads/2022/10/2022-Deloitte-NASCIO-Cyber-Study.pdf
6. https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/2022-state-of-city-county-it-national-survey.pdf?sfvrsn=9b7f8f7_0

ADOBESTOCK SHUTTERSTOCK.COM

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

Sponsored by: Charter COMMUNICATIONS | Spectrum ENTERPRISE™

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions, Internet access, Ethernet access and networks, voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, enterprise.spectrum.com.