DTS
Changing business.
Delivering results.

Comparing Self-Managed Cybersecurity to Managed Services

Choosing to manage your cybersecurity program in-house takes careful consideration and dedicated personnel. As a cybersecurity services provider, DTS helps small and medium-sized businesses (SMBs), especially those involved in government contracting, explore their options, and provides the framework and support for success.

The process of keeping up to date with security vulnerabilities typically involves:

- Collecting and analyzing data to identify changes to the network or unusual behavior
- Drawing on threat intelligence to pick out the latest risks
- Deciding the specific types of behavior that require attention
- Taking action before threats become a security incident
- Generating detailed network security reports for compliance purposes
- Creating cybersecurity policies to inform network configuration and guide the cyber hygiene of employees

Compliant security management, needed to maintain CMMC Certification or other standards and controls, requires multiple people for monitoring, logging, and objective auditing. At a minimum, three people should be designated as Key Personnel, regardless of the company's size, for ethical objectivity. These Key Personnel should be experienced in network monitoring and well-versed in the controls and control enhancements necessary for certification. Staying up-to-date on the evolving requirements and industry best practices is critical. Additional tasks for Key Personnel include configuration management, training, and incident response.

Your responsibilities for a self-managed program

- Interpret and maintain compliant controls
- System monitoring, vulnerability scans, and logs
- Review of auditing logs
- Tailor Systems Security Policy (SSP), policies, procedures, and Plan of Action & Milestones (POA&M) as needed
- Review and update documentation (SSP, Incident Response Plan, Change Board meeting minutes)
- Ongoing configuration management including security access
- Respond to security incidents
- Staff training
- Maintain compliance records for recertification
- Certification assessment

In support of these self-managed activities, DTS offers our CISSP-certified staff, a broad selection of network and security support services, and a consultative and education-oriented approach. Working with your in-house team, we can establish a compliant network, train Key Personnel, determine and direct remediation actions, and provide independent auditing. Once established as a client, DTS is also available for ad hoc contract work.

In-House or Managed: Which option is right for you?

The decision to self-manage often comes down to size and cost. While growing companies might envision saving money by handling security tasks themselves, few are really ready to invest in the personnel and training costs necessary to stand up a team. This is particularly true when Managed Services support for most SMBs is available from experienced vendors like DTS—for less than the cost of one IT professional's annual salary and benefits.

We know that cost—not security—is often a driving factor in cybersecurity decisions. That's why we offer customized managed services rather than fixed-price packages as an option. You only pay for the services your company needs or cannot provide itself.

Our augmented approach allows companies to begin to self-manage some aspects of their security, like daily monitoring or taking part in their Incident Response. It also minimizes many of the risks associated with self-monitoring:

- **Overtaxed Key Personnel:** Failing to complete all daily and weekly monitoring and logging tasks or failing to implement security patches quickly
- **Misinterpretation of CMMC controls:** With 110 controls and 320 assessment objectives, being compliant with NIST 800-171 requires expertise and significant documentation
- **Delayed response to an attack:** The confidence to contain and remediate threats as soon as they are detected.
- **Evolving threats:** Cybercriminals are always finding new ways to get around defenses, and small businesses are particularly at risk for ransom attacks and learning attacks, where your system is used as a testbed. It's critical to stay on top of news and industry best practices.

MANAGED SERVICES. EXCEPTIONAL RESULTS.

DTS offers fully managed network and cybersecurity services for those who want to avoid the risk and responsibilities themselves. Combining the roles of Managed Network Services (MNS) and a Managed Security Service Provider (MSSP), our services deliver value, with an eye for continual improvement, and operational efficiency. Tap our expert team for full-service support, help with specific IT and cybersecurity tasks, or fulfilling the roles of required Key Implementation Personnel.

Add DTS to your team. Call to discuss your security posture and get an estimate for the managed cybersecurity services you need.

Work directly with DTS experts

Our certified professionals work with you, explaining the services we provide and your system performance while driving security through careful monitoring and logging, more efficient processes, and more secure policies. With a predictable fee and access to expertise and top solutions, our managed network and cybersecurity services can make your business run better.

DTS experts certified as:

CISSP® Certified Information Systems Security Professional

CCSP® Certified Cloud Security Professional

Cisco Certified CCNA

C|EH Certified Ethical Hacker

CMMC-AB

CMMI

PMI Project Management Institute.

ISO 9001

6σ

Contract vehicles:

GSA Schedule IT 70 Contract Number: GS-35F-137DA
GSA PSS Contract Number: 47QRAA19D006Q
FAA eFAST

Primary NAICS 541330, 541511, 541512, 541611, 541614, 541990, 611420, 611430

SDVOSB Privately Held Service-Disabled Veteran-Owned Small Business (SDVOB)

GSA Contract Holder

DTS

571.403.1841
sales@consultDTS.com
www.consultDTS.com

3033 Wilson Boulevard
Suite 700
Arlington, VA 22201