CONNSTEP
a CBIA affiliate

PART OF THE MEP National Network™

Managed Service Provider Evaluation & Selection Criteria

A Guide to Help Small & Medium-Sized Manufacturers Achieve Cybersecurity Compliance with the Right Partner

Table of Contents

Introduction

Cybersecurity compliance is often a mandatory requirement, especially for manufacturers contracted as a supplier for the U.S. Department of Defense (DoD). The difficulty for many small and medium-sized manufacturers (SMM), who want to achieve and sustain cybersecurity compliance, is not having adequate information technology (IT) resources on staff or an outside vendor with the necessary credentials and capabilities.

A **managed service provider (MSP)** can not only help an organization improve its cybersecurity capabilities but also improve its IT operations. In order to properly determine which MSP best meets the needs and requirements of your organization, particularly those in the DoD supply chain, this whitepaper provides evaluation and selection criteria to assist you in your decision-making process.

Criteria Development

The guidance provided in this whitepaper has been developed by CONNSTEP, Connecticut's Manufacturing Extension Partnership (MEP) Center, which is part of the National Institute of Standards and Technology (NIST) MEP national network (MEPNN). The criteria for assessing an MSP is based on:

- **the results of a project involving interviews and collaboration with 82 SMMs by the California MEP Center, California Manufacturing Technology Consulting (CMTC)**
- **CONNSTEP's work with hundreds of Connecticut manufacturers building cyber resiliency in the DoD supply chain**
- **expertise and shared best practices of the MEP national network supported by the DoD**

The objective of the initiative was to develop a procedure, plan, and guidance for SMMs on evaluation methods for effective selection of IT and/or security service providers to help assure security and cybersecurity compliance.

Benefits of Hiring an MSP

Hiring a managed service provider can help upgrade the IT operations of an organization. **Many smaller companies have limited in-house IT capabilities and view an MSP's service offering as a way to obtain IT expertise or supplement their in-house IT staff.** MSPs can be used for a range of services, from managing a wide variety of network devices to supporting a specific system.

Despite their advantages, **managed service providers may also come with challenges, especially as the SMM embarks on a cybersecurity compliance journey.** The SMM must be careful of what it is outsourcing, where it retains control of the information, and how it is positioned to part ways with the MSP if their services no longer continue to provide value.

Considerations when Selecting and Partnering with an MSP

Not all MSPs have the same focus on security or can provide required cybersecurity measures. **Many cybersecurity frameworks demand the IT department follow coordinated procedures, provide documentation, and systematically share reports.** If the MSP cannot provide those as a standard operating internal procedure, then your partnership will not produce the necessary results.

Unfortunately, **some MSPs use their client's need for developing cybersecurity controls as an opportunity to upsell technology or services** while not understanding the important role they need to play and the tasks they need to perform to adequately support their clients on their path to cybersecurity compliance. Partnering with the right MSP can make a significant difference.

Understanding MSP Types, Categories, and Expertise

A Managed Service Provider is a third-party company delivering Information Technology services via ongoing and regular management, support, and active maintenance administration on customers' premises, in their MSP's data center such as hosting, or in a third-party data center. **MSPs may deliver their own native services** in conjunction with other providers' services (for example, an MSP can provide system administration management on top of a third-party infrastructure as a service [IaaS] platform).

Frequently, the MSP will only work with technology that they know, or technology of manufacturers they partnered with, potentially limiting the solutions they offer to that specific technology, and not necessarily what is the best approach based on their client's situation and needs.

Most IT MSPs develop a specialization or expertise in certain functions, but there are MSPs that still provide just the core offerings of a network, infrastructure, and basic break/fix support services (reactive rather than proactive).

Specializations

Some MSPs embrace specializations in specific segments of IT with a hybrid delivery approach, contracting work above cost with other specialized technology providers such as Azure cloud-based infrastructure services, cloud data storage or backup technology, or Microsoft Office365 technology to name a few.

Market Focus

Other MSPs focus on specific vertical markets, such as legal, financial services, healthcare, or manufacturing.

Managed Security Service Provider (MSSP) is a third-party firm exclusively offering specialized types of security services, such as remote firewall administration and monitoring and other security-as-a-service offerings.

Additional Expertise and Services Offered by Some MSPs

Network Operation Centers (NOCs)

NOCs are typically centralized locations where the network operation staff provides 24x7x365 supervision, monitoring, and management of the client's network, servers, databases, firewalls, devices, and related external services.

Different models include:

- Virtual System Administration (one or two staff members who do most of the work on your account)
- Help desk/ticketing system - whoever is available at time of inquiry, not consistent

Security Operation Centers (SOCs)

SOCs are a dedicated security team that monitors and analyzes activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for reporting on security risks.

Capabilities include:

- Conduct threat assessments (scans, penetration tests)
- Monitor audit logs and provide alerts (Security Information and Event Management [SIEM] products)
- Can be a good complement to in-house IT staff

Managed Detection and Response (MDR)

MDR is an outsourced cybersecurity service that combines technology and human expertise to perform threat hunting, detecting, and responding to advanced threats, breaches, or cybersecurity incidents. It helps rapidly identify and limit the impact of cyber threats, performs forensic investigations and data analysis, guides response and remediation.

Applications Support

Applications Support is a service that reinforces the maintenance and development of applications. It may oversee the installation of software applications, optimize application performance, install updates, and perform debugging procedures. In addition, it ensures the applications supporting operational processes in a business run smoothly and enable users to conduct their business.

Database (DB) Support

DB Support ensures that customer databases are protected and monitored by providing a secure database environment, monitoring database performance and improving efficiency, and establishing backup and recovery procedures. It may also include data migration and reporting support.

Virtual Chief Information Officer (vCIO) or CIO advisory

The **vCIO** role provides experienced IT leadership as an additional resource to assist your organization in making decisive IT investments and ensuring your IT staff has the right sense of urgency and direction. This role should not be an account management function but instead fulfill a client's strategic IT guidance responsibilities.

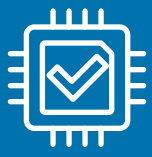
Conclusion for SMM on Selecting IT/Cyber MSP

There are many criteria for selecting an IT MSP. A measured analysis of what the MSP can do, how the partnership will work, and how the MSP will support SMM cybersecurity efforts is needed to select the most suitable IT MSP for your organization. **A formalized process should be conducted to interview, select, bid, and contract with a provider that will support the SMM's strategy, goals, and initiatives.**

About CONNSTEP A member of the MEP National Network, CONNSTEP is a manufacturing consultancy firm serving small and medium-sized companies, implementing advanced business and technical solutions, and workforce strategies, that help organizations grow, improve profitability, and create sustainable competitive advantages. **You can contact CONNSTEP's team for assistance on this MSP selection process.**

Appendix

38 Essential Questions & Inquiries for Selecting an MSP



Discovery:

1. Describe the SMM's program needs. Discuss and agree internally on your organization's needs when it comes to the IT provider service offerings:

- Establish expectations of the relationship
- Identify any specialized technology needs
- Build a matrix of service wants/needs

Technology:

2. Review the technology and architecture that the provider can offer the SMM and any of their subcontractors – can the SMM's technical needs be met?

3. What is the provider's expertise and areas of weakness? Have they developed any additional services, and what is the level of their experience/credentials of that service?

4. Determine if the provider has an NOC, is the service delivered via Remote Monitoring and Management (RMM) tools, and are there dedicated engineers to support your network, information systems, and endpoints.

5. Does the provider have a purpose-built technology or rely on third-party technology to support the SMM?

6. Review cloud-based offerings that the provider has and examine related inherent risks for the SMM.

7. Review the data recovery/backup options, can the provider support alternate processing site for business continuity and disaster recovery planning.

8. Determine if customization of MSP technology/solutions is needed.

9. Review the help desk service model and options that the provider can provision to the SMM. Does the provider assign dedicated technicians and engineers to their client's accounts?

10. Review the "User Experience" – does the provider have a single interface dashboard for IT/security technologies that the SMM can use?

11. Assess the provider's Service Level Agreement (SLA) and Customer Relationship cadence of meetings.

12. Include cybersecurity incidents and investigations in the Service Level Performance Agreement (include timing).

13. Define actions to be taken when service issues arise (additional run books/playbooks?).

14. Identify warranties/performance penalties/changes in business conditions.

15. Define the duties of the IT provider and the SMM (who does what/when, e.g. security incident management).

16. What are the hours of service (9-5 vs 24x7)? Given that security is typically 24x7, will the MSP vendor adopt a follow the sun model or use an emergency on-call system?

17. Review onboarding time and related costs.

Costs:

18. Perform a cost comparison with features between multiple MSPs.

19. Examine cost factors – does the provider provide "budget-friendly" options for the SMM?

20. Measure the financial stability of the provider, length they've been part of this practice, their future vision and roadmap for services.

Security:

21. What is the provider's market focus and does it match the SMM's industry?

22. Determine the provider's cyber security experience (past clients/projects, size, complexity, technology).

23. Evaluate expertise - does the MSP have expertise and experience in industry-specific requirements and security compliance practices? Which ones? How many clients have implemented NIST 800-171/CMMC?

24. Review and compare cyber services and expertise offered between prospective providers (e.g. "monitored events" logs/SIEM, etc.)

25. How will the MSP be able to coordinate your custom audit logs from various network devices into MSP's security monitoring system? What reports/visibility to the security events will the SMM have and what will be the timing of receiving this information?

26. If working with MSSP or another security vendor, is the vendor able to open help tickets with the IT MSP for the SMM's network/firewall systems security vulnerabilities and issues?

27. Determine the data flow between the SMM and the IT provider – is CUI shared? Are appropriate protections in place? What cybersecurity controls does the IT provider have implemented and are those documented and maintained?

28. Does the MSP understand the SMM's required security procedures and have a standard operating internal procedure designed to support SMM's policies and procedure requirements (e.g. SMM custom procedures support, information systems documentation, and systematic reports)?

29. Will this partnership lead to co-management of the cybersecurity devices/systems or delegate management to MSP? Is the SMM aware of the visibilities/restrictions/timeliness and responsibilities that this will create?

30. Will the MSP need access to network or other devices in order to correlate cybersecurity risk assessment? Is this risk assessment included in your cost estimate?

31. How will the MSP help the SMM during the audit period? Are they fluent in the required audit technology documentation?

32. Has the MSP done a self-assessment against NIST 800-171? Review the provider's security policies and what security practices they have in place in their own company. Are their employees trained in those practices?

Best practices, culture, and customer service:

33. Determine if the provider uses checklists (playbooks, runbooks, SOPs, etc.).

34. Assess the organizational impact – does the MSP set clear expectations about client requirements? (e.g., is onboarding or engaging on a regular basis with the clients a complex task for the SMM?).

35. Assess customer service and evaluate the relationships that the MSP has with other manufacturers (check references). What is the provider's internal company culture like?

36. Determine the location of the provider and affiliates (local, distributed, remote, help desk outsourced, etc.).

37. Evaluate the future growth of your SMM organization – can the MSP grow with the SMM?

38. Define a process for termination/exit strategy.

Please note: The contents in this document should not be construed as an endorsement (written, spoken, expressed, or implied) of any solution, product, service, or methodology.

MEP National Network™

CONNSTEP is the official representative in Connecticut of the **Manufacturing Extension Partnership National Network (MEPNN)**, which is part of the **National Institute of Standards & Technology (NIST)** a U.S. Department of Commerce agency.

The MEP National Network is focused on helping small and mid-sized manufacturers generate business results and thrive in today's technology-driven economy. The MEPNN is comprised of 51 MEP Centers located in all 50 states and Puerto Rico, with 1,400 trusted advisors and experts at nearly 375 MEP service locations, providing U.S. manufacturers with access to resources they need to succeed.

Our mission is to strengthen and empower U.S. manufacturers.

Contact CONNSTEP to initiate the IT MSP evaluation and selection process for your business.

CONNSTEP
a CBIA affiliate

350 Church Street, Hartford, CT 06103

(800) 266-6672

info@connstep.org

https://www.connstep.org