Choosing the Right Managed Service Provider for CMMC

For contractors seeking Cybersecurity Maturity Model Certification (CMMC) selecting the right Managed Service Provider (MSP) is essential to ensure senstitve data is protected, cybersecurity standards are met. The CMMC v2.0 proposed final rule, published December 2023, requires External Service Providers (ESPs) to achieve CMMC compliance at or above the required level of their clients. This checklist is designed to help you evaluate whether an MSP is prepared to support you through CMMC.

Question?	Yes	No
CMMC Awareness & Readiness		
Has the MSP asked about your current efforts toward CMMC compliance?	☐	☐
Does the MSP offer references or have other CMMC clients they are actively supporting?	☐	☐
Has the MSP already conducted their own NIST SP 800-171 rev2 Self Assessment, developed a Plan of Action & Milestones (POAM), and drafted a Systems Security Plan (SSP)?	☐	☐
Does the MSP partner with a Cyber Accreditation Body (AB) Registered Practitioner Organization (RPO) with Certified CMMC Professional(s) (CCP) as part of their team to provide CMMC gap analysis and readiness support?	☐	☐
Does the MSP offer a Shared Responsibility Matrix (SRM) aligned with NIST SP 800-171 rev2 controls and objectives?	☐	☐
Does the MSP offer policy & documentation development support, including support for evidence collection and management?	☐	☐
CMMC Compliant Technical Support Services		
Access Control Implementation		
Does the MSP use MFA to access client information systems?	☐	☐
Does the MSP implement and manage role-based access controls to ensure that only authorized personnel have access to Controlled Unclassified Information (CUI)?	☐	☐
Does the MSP Deploy MFA across critical systems to strengthen authentication processes in line with CMMC requirements?	☐	☐
Network and Data Security		
Does the MSP implement encryption for data at rest and in transit to protect CUI?	☐	☐
Does the MSP design and manage secure network architecture to segregate sensitive data and control data flow within the organization?	☐	☐
Does the MSP configure and maintain firewalls and VPNs to secure remote access and protect against external threats?	☐	☐
Vulnerability Management and Patching		
Does the MSP perform weekly or regular vulnerability scans on systems to identify and assess security weaknesses?	☐	☐
Does the MSP ensure timely application of security patches and updates to mitigate vulnerabilities?	☐	☐
Does the MSP develop and implement a plan to address identified vulnerabilities, ensuring compliance with CMMC risk management practices?	☐	☐
Security Monitoring and Incident Response		
Does the MSP provide 24/7 monitoring of networks, systems, and endpoints to detect and respond to potential security incidents?	☐	☐
Does the MSP deploy and manage SIEM tools to aggregate and analyze security logs, providing real-time alerts for suspicious activities?	☐	☐
Does the MSP develop and maintain an incident response plan tailored to CMMC requirements?	☐	☐

Be sure of your decision before committing to a contract!

Question?	Yes	No
Does the MSP coordinate and support incident response activities, including investigation, containment, and reporting?	☐	☐
Data Backup and Recovery		
Does the MSP implement automated backup processes to ensure regular backups of critical data, including CUI?	☐	☐
Does the MSP's backup solution use FIPS-validated cryptography stored with a FedRAMP Moderate or equivalent cloud service provider?	☐	☐
Does the MSP develop and test disaster recovery plans to ensure rapid recovery of data and systems in the event of a cyber incident?	☐	☐
Does the MSP provide support for data restoration activities following a security incident or data loss event?	☐	☐
Security Awareness Training		
Does the MSP conduct regular security awareness training tailored to CMMC requirements for all employees?	☐	☐
Does the MSP provide specialized training for IT and security personnel on their specific roles in maintaining CMMC compliance?	☐	☐
Does the MSP run phishing simulation exercises to raise awareness and prepare employees for social engineering threats?	☐	☐
General Costs		
Does the MSP have a straightforward pricing structure?	☐	☐
Does the MSP provide clarity about any "other costs" you may incur beyond the agreement? (ex: compliance support, new hardware / software, etc.)	☐	☐

Be sure of your decision before committing to a contract!