# CMMC PREPARATION Webinars:
# How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance

CONNSTEP
5/4/2023

# CMMC PREPARATION Webinars

CONNSTEP
a CBIA affiliate

**Four Webinar Series**

**3/9 – 6/1**

**12 noon – 1 pm**

| | |
|---|---|
| **March 9th** | Understanding CMMC Timeline & Steps to Compliance |
| **April 6th** | How to Develop & Implement Effective CMMC Policies & Procedures |
| **May 4th** | How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance |
| **June 1st** | Steps to Take in Preparation for a CMMC Audit |

# Webinar #3 Agenda

CONNSTEP
a CBIA affiliate

## How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance

- The Benefits and Challenges of Partnering with IT MSP
- MSP Role in Supporting CMMC Compliance
- The Security Risks of IT Vendors and Mitigation Strategies
- Evaluating and Managing your IT MSP

# Presenters:


**Anna Mumford**
Cybersecurity Consultant

860.305.8880
amumford@connstep.org



**Jeffrey Orszak**
Director, Business Technology and Innovation

860.539.4905
jorszak@connstep.org

# Guidance

Nothing in this presentation (written, spoken, expressed, or implied) is legal advice.

Nothing in this presentation (written, spoken, expressed or implied) should be construed as an endorsement of any solution, product, service, or methodology.

# Poll #1

# Benefits of Hiring an IT MSP

CONNSTEP
a CBIA affiliate

**Benefits of partnering with an information technology (IT) external vendor:**

1. Supplement or replace in-house IT staff
2. Access to IT expertise
3. Improve efficiency for systems support and maintenance
4. Access to a wide range of services/technologies
5. Access to share resources and scalable pricing models

# MSPs Categories

**MSPs can be classified into different types and categories based on their service offerings:**

**Managed Service Provider (MSP)**
provide a wide range of IT services and solutions via ongoing and regular management, support, and active maintenance administration.

(ex. Network implementation, monitoring, and troubleshooting, or IT help desk services)

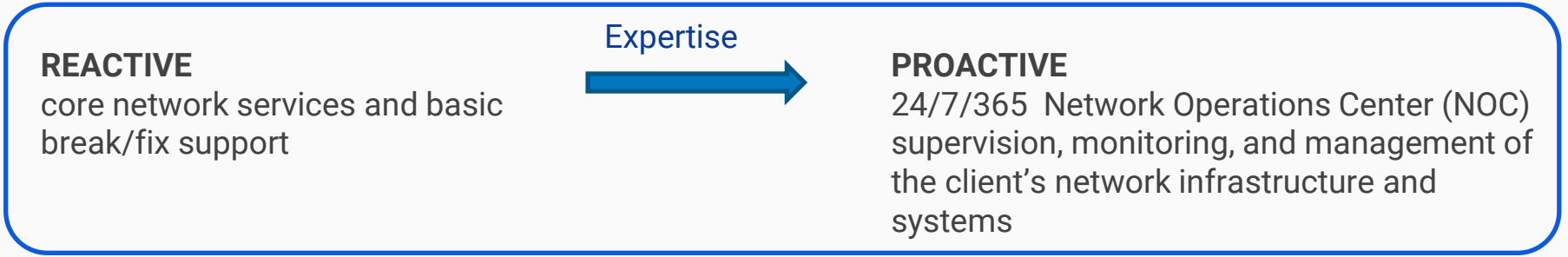
**Managed Security Service Provider (MSSP)**
specialize in exclusively providing security-as-a-service services and security-related solutions, use advanced tools and technologies to protect businesses from cyber threats

(ex. threat detection and response, vulnerability scanning and assessment, pen testing, security monitoring and analytics)

# MSPs Expertise and Specializations

**There is a wide range of:**

- support MSPs can provide and their level of expertise




- technology domains they specialize in or partnered with (ex. MS Office 365)
- specific specializations and skills they develop (ex. MS SharePoint data migration)

# MSPs Range of Services

CONNSTEP
a CBIA affiliate

## General MSP

IT Infrastructure Management

Hardware/Software Procurement

Helpdesk Break/Fix Support

VoIP Systems

Database (DB) Support

## Hybrid MSP

Network Operation Centers (NOCs)

Managed Email

IT Consulting

Backup & Recovery

Virtual Chief Information Officer (vCIO)

Applications Development, Maintenance, & Support

Cloud Computing

## MSSP

Network Monitoring, Breach Detection, & Response

Multi-Factor Authentication

Security Operation Centers (SOCs)

Security Awareness Training

Security Information & Event Management (SIEM)

## Security Firms

Incident Response & Forensic Analysis

Vulnerability Assessment & Management

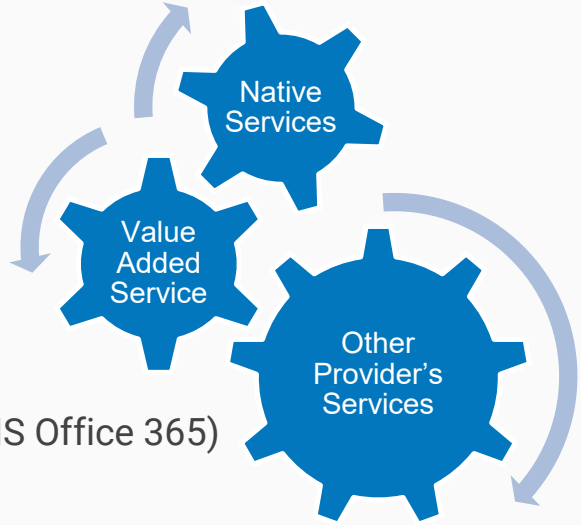
Compliance & Security Audits

Penetration Testing

Cybersecurity Risk Management

Cybersecurity Program Consulting

# MSP Delivery Strategies




**Delivery strategies:**

- Deliver **their own native services**
- Outsource **other providers' services** (ex. Barracuda Cloud backup, MS Office 365)
- Resell **other technologies** (ex. Hardware/software)
- Deliver **their own expertise on top of other providers' services** (ex. migrating data to MS Office 365, managing firewall in Azure)

# MSPs Types and Business Models

CONNSTEP
a CBIA affiliate

**MSP firms may differ in their business models based on the types of services they offer and the industries they serve:**

1. **Vertical MSPs:**
- serving specific industries or verticals (ex. healthcare, finance, manufacturing, legal, retail, etc.)
- expertise in that industry's unique IT challenges and requirements

2. **Horizontal MSPs**:
- provide a broad range of IT services to businesses of all industries and sizes
- may specialize in specific IT domains (ex. network management, cybersecurity, or cloud computing)

3. **Boutique MSPs**:
- focus on providing specialized IT services (data backup/recovery, IT consulting)

4. **Value-added Resellers (VARs):**
- resells hardware and software products and adds value to those products (ex. providing implementation, customization, integration services, training, or maintenance)

# Challenges with it MSPs

CONNSTEP
a CBIA affiliate

**SMMs Challenges with IT MSPs:**


- Frequently, the MSP offers are limited to:
  - the solutions they know, or
  - the technology of manufacturers they partnered with
- SMMs do NOT vet their IT MSPs – do not know the right questions to ask
- SMMs do NOT understand the different IT services and what they are getting vs what they need
- SMMs do NOT know how to delineate IT responsibilities and retain control over data
- SMMs do NOT define Service Level Agreements (SLAs) or scope them well
- SMMs do NOT know how to evaluate cost, how do they compare to other vendors offering similar services, and is the level of service comparable
- The MSPs introduce Security Risks because of weak cybersecurity posture
- How SMM is positioned to part ways with the MSP if their services no longer continue to provide value

# Actions to Take

1. What type of MSP are you working with?
2. List the technologies and services you utilize from your MSP?
3. How your MSP compares with other MSPs in the region?
4. What do you feel are the strengths and weaknesses of your IT MSP?

# Partnering with IT MSP for CMMC Compliance

CONNSTEP
a CBIA affiliate

**MSP has an important role to play in SMM's cybersecurity compliance**
– besides providing technical expertise!

And it is different from what they usually advertise.

-> Having IT expertise does not equal knowing cybersecurity – different skill set!

# MSP Role in Supporting CMMC Compliance #1

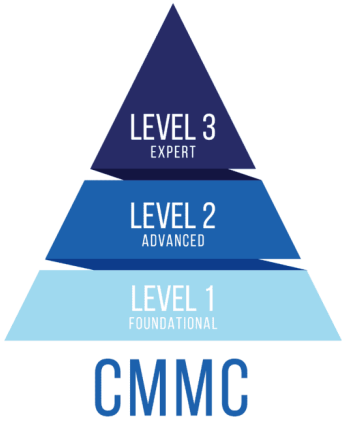
CONNSTEP
a CBIA affiliate

**# 1. Coordinated cybersecurity procedures**

- Develop a process for handling requests
- Keep track of requests (ex. Security setting change, new employee, new printer)
- Provide feedback/documented completion of requests

Example: Employee Termination Procedure

- help desk processes request, schedules user account disablement, sends a confirmation
- executes user account termination on schedule
- information on user termination forwarded to SMM



# MSP Role in Supporting CMMC Compliance #2

CONNSTEP
a CBIA affiliate

**# 2. Provide evidence of compliance/documentation of technical settings**

- Cloud Backup (ex. where it's physically stored, cryptography in-flight/at storage, physical access controls documentation, etc. )
- Network monitoring alerts/responses (ex. Who performs monitoring, conditions for alerts/severity categories, the response notification policy/SLAs)
- Documentation on MSP training on handling CUI/compliance practices
- Documentation of security settings and change management (ex. AD Group Policy settings, configuration change backout plan and security impact assessments, usage of baseline configurations)

# MSP Role in Supporting CMMC Compliance #3

CONNSTEP
a CBIA affiliate

**# 3. Provide monthly reports and regular reviews**

- Generate automated reports on all systems' status, activities, and any change requests by category
- Hold monthly/quarterly regular reviews of reports and change control logs, and any suspicious activities
- Perform periodic risk assessments and analysis, discuss findings
- Provide IT oversight and not governance

Please note: No one person or vendor should have complete control over a critical process or function -> the principle of separation of duty.

# Understanding the Delineation of Responsibilities

CONNSTEP
a CBIA affiliate

**There should be a clear division of responsibilities between MSP and the company:**

**MSP responsibilities** (ex. network information systems and devices, cloud computing, and backup)

**vs.**

**Business Security responsibilities** (ex. physical, personnel, OT including IoT and Edge Computing, ICS, business processes, risk assessment and acceptance, power and connectivity, strategy and governance)

**You cannot transfer your cybersecurity risk or responsibility to your IT MSP or any other vendor – you can only manage and mitigate it!**

# Conclusions

**MSP needs to have:**

1. The capabilities to provide the documentation (ex. the tools to keep track and generate automated reports)
2. The internal standard operating procedures (SOP) to perform required activities on a regular and consistent basis
3. Thorough documentation of their services and SLA

**SMM needs to :**

1. Understand clear delineation of responsibilities
2. Define the roles and responsibilities of the MSP in compliance efforts and ongoing risk management
3. Ensure adequate visibility and oversight over the systems, data, and IT vendor's activities

# Poll #2

# Security Risks of IT Vendors

CONNSTEP
a CBIA affiliate

**Third-party providers, especially IT vendors, pose a significant cybersecurity risk to organizations:**

MSP vendors have administrative access to many clients' systems

MSPs are a frequent target for hackers

If MSP security is compromised, it can have a devastating impact on the organization's operations and data security

# Security Risks of 3rd Party Providers


**MSP vendor's cybersecurity risks:**

- Absence of security controls and measures in place
- Outsourcing services to a 3rd party providers that:
  - operate outside of MSP's direct control (ex. cloud providers)
  - may not be compliant with the DFARS regulations or standards
- Their employees could intentionally or accidentally access sensitive systems or leak confidential information
- MSPs may accidentally introduce malware through infected software or devices

# Vendor Risks Addressed in Compliance Requirements

- **Specific MSP vulnerabilities addressed in NIST SP 800-171:**

- Multi-factor authentication
- Remote access sessions encryption
- Remote access support and maintenance activities authorization and supervision
- Access control for the administrator account
- Least privilege principle
- Storage of unencrypted passwords/password sharing
- Flow down the DFARS requirements to your MSP, if they store CUI
- Personnel security

# Risks Mitigation Strategies Associated with MSPs

CONNSTEP
a CBIA affiliate

**Strategies to reduce Cybersecurity risks associated with MSP vendors:**

- conduct a risk assessment of your MSP
- define and communicate your security requirements for your MSP (ex. encryption, access controls)
- include security-related provisions in MSP contracts, including:
  - annual security audits and periodic security reviews
  - breach notification and risk assessment performance
  - liability provisions for breaches that occur as a result of the vendor's negligence or failure to meet security requirements
- continuously monitor MSP to ensure they are meeting security requirements

# Summary: Evaluating and Managing your IT MSP

CONNSTEP a CBIA affiliate

## How do you evaluate or select an MSP vendor that is well-suited to support your cybersecurity program?

**Gain an understanding of their:**

- expertise and experience in assisting SMMs with the DFARS requirements (specializations and market focus)
- technology and other services that MSP provides and the inherent risks of those technologies (ex. Infrastructure in the cloud: IaaS)
- cybersecurity posture of your IT MSP and their risk management processes
- capability to support clients with DFARS requirements (ex. coordinating procedures, and reports)
- specific services required to support DFARS requirements (RMM vs SIEM)
- ability to assist during a security incident forensic investigation

# Asking MSP the Right Questions

## Know what questions to ask:

**Technology**

- What type of support do they offer (break/fix or NOC support)
- What expertise do they have and what technology domain do they specialize
- What services do they offer and do those include cybersecurity offerings
- What specific tools and technologies do they use to support CMMC requirements
- What qualifications and certifications do their consultants and engineers hold
- Do they outsource their services and if so, to whom (documentation)

**Experience (vertical)**

- What industries do they serve
- Discover their experience in handling industry-specific requirements
- How do they meet the unique industry challenges
- Provide examples of similar organizations they worked with to achieve CMMC compliance

# Asking MSP the Right Questions

**Cost Comparison**

- How do costs of services compare to other vendors offering similar service
- Is the level of services comparable
- Are there additional service onboarding costs

**Providing Security – Best Practices**

- What are the IT MSP cybersecurity posture, and their risk management processes
- How do they handle the coordination of processes, keep track of requests
- Do they provide monthly activities/status reports  and offer regular security reviews
- Can they provide documentation proving technical compliance with requirements

**Internal Security Posture, Practices, and SOPs**

- Would you be able to provide documentation on a 3rd party security audit and risk management process
- Do their employees receive regular training on security best practices and handling CUI

# Evaluating and Managing your IT MSP

**Additional provisions to review in contract/SLAs with MSP:**

- Assistance in regular cybersecurity audits
- Incident response plans testing and incident response participation
- Breach notification and response procedures
- Liability provisions for security incidents as a result of MSP's negligence/failure to meet security requirements

# Actions to Take

1. Download: A Guide to Help SMMs Achieve Cybersecurity Compliance with the Right IT MSP Partner - https://bit.ly/msp-guide
2. Use the guide to assess your partnership with your IT MSP

# State Funding Available

State funding is available for

**Connecticut Manufacturing SIRI and CYBER Assistance Program (SAC)**

for manufacturing companies or allied service providers located in Connecticut.


https://ctsac.ccat.us/

CONNSTEP
a CBIA affiliate

# Questions?

CONNSTEP
350 Church St., Hartford, CT 06103 | 800.266.6672
CBIA & Affiliates | cbia.com | connstep.org | readyct.org

PART OF THE MEP National Network™
Connecticut Department of Economic and Community Development

# Glossary

CMMC – Cybersecurity Maturity Model Certification
CUI - Controlled Unclassified Information
DFARS - Defense Federal Acquisition Regulation Supplement
DIB – Defense Industrial Base
DIBCAC – Defense Industrial Base Cybersecurity Assessment Center
DCMA – Defense Contract Management Agency
IRP – Incident Response Plan
IT – Information Technology
MEP - Hollings Manufacturing Extension Partnership
MSP – Managed Service Provider
MSSP – Managed Security Service Provider
NIST – National Institute of Standards and Technology
NIST SP 800-171 – NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
POAM – Plan of Action and Milestones
SPRS – Supplier Performance Risk System
SSP – System Security Plan