“Your MSP, You, and Compliance”

How To Know Your If MSP Will Actually Help Or Hurt You
In Achieving CMMC Compliance

Presented by:

Leia Kupris Shilobod, CCP, CISM

CompliancyIT

CMMC IT Documentation Compliance Toolkit

CompliancyIT

Why Are We Even Talking About MSPs?

- Percent of companies using an MSP to support at least some of their infrastructure
  - **90%**
- Businesses rely on these 3rd Parties
  - Get help with day-to-day support
  - Augment existing staff to get infrastructure up
  - Solution environments that are compliant
  - Selection and monitoring of security tools
  - Aide in compliance

Why Are We Even Talking About MSPs?

- Technical controls can be confusing and frustrating to understand
  - Get a technical person to assure it’s implemented properly
  - They likely don’t know how to implement the controls effectively EVEN IF THEY SAY THEY DO
- You expect your MSP to be knowledgeable and just do “the things”
  - People make mistakes
  - People forget
  - There is little room for error in a CMMC Assessment
  - As little as .3% of the 320 Assessment Objectives = NOT MET means FAILURE

Why Are We Even Talking About MSPs?

And if all that wasn't enough to make you think about who you choose as your partner….

Now MSPs need to be compliant, too

MSPs Must Be Compliant

§ 170.19 CMMC scoping.

(2) If the OSA [OSC] utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP **must have a CMMC Level 2 Final Certification Assessment**. If the ESP is internal to the OSA [OSC] , the *security requirements implemented by the ESP should be listed in the OSA's [OSC's} SSP* to show connection to its in-scope environment. In the CMMC Program, CUI or **Security Protection Data** (*e.g.,* log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.

4 Quick Promises:

- The 4 key things your MSP MUST be doing to assure you don’t FAIL compliance
- Turn your heels and RUN if your MSP says this ONE thing
- How to tell if your MSP is worth what you’re paying them
- How to find a GOOD MSP that will get and keep you compliant

CompliancyIT

Who Is Leia Kupris Shilobod And Why Should You Listen To What I Have To Say?

- Founded InTech Solutions / CompliancyIT as a **Security focused MSP in 2006**
- Implementing NIST 800-171 for companies **since 2017**
- Have helped **over 200** organizations with their CMMC compliance programs and documentation
- **Speak country-wide** on IT Security, IT Documentation, IT Operations, CMMC | NIST 800-171, and IT for Manufacturers
- CIT is a **CMMC RPO**, Leia is a Certified CMMC Professional (**CCP**), and Certified Information Security Manager (**CISM**)
- Creator of the **"CMMC IT Documentation Toolkit"**

CISM

CAICO CERTIFIED CMMC PROFESSIONAL

CYBER AB CMMC CERTIFICATION REGISTERED PRACTITIONER ORGANIZATION RPO

The 3 Indisputable Rules
Every Manufacturer Needs To Know Before Buying Any Technology Service or Product
A Manufacturer's Guide to Purchasing IT Products & Services

CompliancyIT

Why This Is Absolutely Vital NOW

URGENT

- The CMMC Rule is going final in **Winter 2024/2025**
- It will affect **DoD contractors**, their **supply chain**, **MSP's**, and **MSSP's** alike
- The controls are not **prescriptive**
- If actions are not performed on a regular basis, AND documented, **you've not implemented CMMC**

CompliancyIT

Why Do We Need MSPs Anyway?

- Vet security tools and interact with vendors
- Assure regular maintenance is completed on the information systems
- Provide day to day support
- Have specialized knowledge in standing up servers, firewalls, networks, M365/Google environments, and security toolsets
- Can save hundreds of hours, tens of thousands of dollars, be more efficient and more effective than in house

CompliancyIT

The Thing You Have To Understand About What You’re Getting From Your MSP

- No MSP contract is exactly alike
- What you actually get for different named services can be confusing (e.g. – ‘vCIO’)
- Many MSPs tie you into 3 year agreements – don’t get stuck!
- Most MSP’s don’t offer you a Shared Responsibility Matrix (SRM)
- Unclear about what compliance-related services are included… and what’s going to cost more
- Are you sure they are onboard with getting compliant themselves?

CompliancyIT

CMMC is a PROGRAM

- There is no “finish line”
- POAM remediation is only the START
- “Safety Program,” “Quality Program,” “QA Process”
- Specific activities: Daily, Weekly, Monthly, Quarterly, Yearly
- Evidence collection over time
- Updating documentation: POAM, SSP, Policies, Plans, Procedures, Lists, etc.

No One Person or IT Company Can Do It All

- No abdicating your CMMC Compliance to an outside organization
- Collaboration is necessary to assure GOOD IT documentation
- Assure you have a Shared Responsibility Matrix (SRM) in place
- Informs who should be responsible for what kind of documentation and clarifies what information needs to be shared to have accurate documentation

CompliancyIT

THE IMPERATIVE OF A SHARED RESPONSIBILITY MATRIX (SRM) FOR COMPANIES IN THE DOD SUPPLY CHAIN

Provided by:
Leia Shilobod, CISM, CCP
Chief Security Officer
CompliancyIT
www.compliancyit.io
724.235.8750

There Are “Bad Eggs” Out There

- If they say “no problem, we’ve got all things CMMC covered for you!” Run away FAST.
- Some MSPs see the opportunity (READ: $$) and will say whatever it takes to get you to sign a contract
- Even the engineers at MSPs are unsure about what the controls ACTUALLY mean!
- “Wham, bam, thank you, ‘mam” Gap Assessments
- “CMMC In A Box”

CompliancyIT

MSPs Are An Unregulated Industry

- Have been around for 40 years
- No official standards
- No regulatory body or required certifications
- No education required
- MSPs who serve the DIB will be the first regulated MSPs in history
- ***About time, right?***

But, They've At Least Got The Technical Stuff Handled, Right?

- If you're not technical, how do you know if the technical configurations, technical documentation, or security tools are adequate?
- Many MSPs don't understand what kind of documentation is required
- Environments are used DAILY – which means they can go out of alignment (compliance) DAILY
- If there is no clear Daily, Weekly, Monthly, Quarterly, Yearly cadence and no accountability, how do you even know what's ACTUALY happening?

CompliancyIT

REMEMBER: You Will Be Signing The Attestation

- § 170.22 **Affirmation.**
- (a) *General.* The OSA must affirm continuing compliance with the appropriate level CMMC Self-Assessment or CMMC Certification Assessment. The **affirmation shall be submitted in accordance with the following requirements:**
- (1) *Affirming official.* All CMMC affirmations shall be submitted by the **OSA senior official who is responsible for ensuring OSA compliance with CMMC Program** requirements.
- (2) *Affirmation content.* Each CMMC affirmation shall include the following information:
  - (i) Name, title, and contact information for the affirming official; and
  - (ii) Affirmation statement attesting that the OSA **has implemented and will maintain implementation** of all applicable CMMC security requirements for all information systems within the relevant CMMC Assessment Scope at the applicable CMMC Level.
- (3) *Affirmation submission.* The affirming official shall submit a CMMC affirmation in the following instances:
  - (i) Upon **completion** of the assessment (conditional or final);
  - (ii) **Annually** thereafter; and
  - (iii) Following a **POA&M closeout** assessment, as applicable.

You Need A System Of Accountability

- Start with an SRM
- Assure clear Compliance Actions Cadence (for YOU and your MSP)
- Policies, Plans, and Procedures must be functional and understood by both parties
- Regularly scheduled meetings to report on activity and compliance status
- Regular pulse for reviewing and updating documentation (POAM, SSP, Policies, Plans, Procedures, Lists)

Pulling It All Together

- Get a Letter of Intent that your MSP is implementing the controls NOW and that they intend on certifying
- Secure and feel comfortable with the SRM BEFORE entering into an Agreement
- Don’t roll into a $25K - $75K assessment with the risk and the stress unless you have clarity
- Assuring BOTH your operational and technical documentation is solid is KEY
- Having a system to assure your SSP and other supporting documentation is up to date and being USED is vital
- Regular Security Assessments are providing you with assurance the controls are implemented effectively
- Risk Assessments are tracking the success of your CMMC Cybersecurity Program so you can make changes or pivots when necessary
- Your robust CMMC Cybersecurity Program is not only getting and keeping you compliant – it’s showing you RESULTS

CompliancyIT

You’re Probably Wondering ‘What Do I Do Next?’

- Demand a Shared Responsibility Matrix
- Get a Letter of Intent from MSP to get compliant
- Review your Agreements to understand if compliance is included
- Create a Compliance Actions Cadence
- Start regular pulse for reporting actions, alignment, and updating documentation

Crazy Offer To Help You

You can access our
18 years of experience being an MSP,
knowing **hundreds of MSPs** and their
services, and in implementing and
maintaining **effective**
CMMC Cybersecurity Compliance Programs
absolutely FREE

CompliancyIT

Free, 3rd Party
MSP Suitability Review

In 60 Minutes we will:

- Review and demystify your current agreement
- Review the Shared Responsibility Matrix to determine if its clear, complete, and you understand your responsibilities
- Help you understand what, if any, compliance services are in scope
- Check backup and security stack for suitability

MSP Suitability Review

- We’ll bring our years of experience as an MSP, and knowing hundreds of MSPs to show YOU where your gaps are, or give you peace of mind you’ve got a solid MSP
- Guarantee your 60 minutes will be valuable and walk away with greater clarity
- If after our 60-minute call you think it was a total waste of your time, I will donate $500 to the charity of your choice

CompliancyIT

60 Minute MSP Suitability Review

- Claim your consult NOW by **emailing**: info@compliancyit.io
- **Subject:** MSP Review
- OR stop by the CompliancyIT booth
- We will schedule your consult in the next 14 days

CompliancyIT

The Challenge

- I can only offer the MSP Suitability Review **for 9 companies**
- They have to be scheduled by the end of CUI-CON

60 Minute MSP Suitability Review

- Claim your consult NOW by **emailing**: info@compliancyit.io
- **Subject:** MSP Review
- OR stop by the CompliancyIT booth
- We will schedule your consult in the next 14 days

CompliancyIT

QUESTIONS?

“Your MSP, You, and Compliance

Leia Kupris Shilobod, Founder and Chief Security Officer, CompliancyIT
Author | Speaker | IT Princess of Power
Leia@compliancyit.io
www.compliancyit.io
724.235.8750.land
www.linkedin.com/PrincessLeia