The CMMC Certification Assessment:
A Behind The Scenes Look

Presented by:
Leia Kupris Shilobod, CCP, CISM
CompliancyIT
Cybersecurity Compliance Toolkit

CompliancyIT

Today We're Going To Cover:

- Tips on **writing an SSP** that demonstrates your proper implementation of the controls
- What to expect for **assessor questions**
- How to **prep your team** to respond to assessor questions
- How **documentation** can make or break your assessment – and what to watch out for
- How to **advocate** for your implementation of the controls and program

CompliancyIT

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

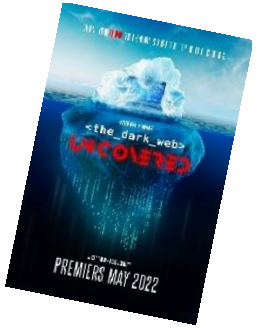
"I am a cyber security, documentation, and compliance professional who specializes in helping companies to **standardize** and **secure** their **IT infrastructure and processes** for companies with less than 2,000 endpoints."

- Founded InTech Solutions / CompliancyIT as a Security focused MSP in 2006
- Speak country-wide on IT Security, IT Documentation, IT Operations, CMMC | NIST 800-171, and IT for Manufacturers
- Teaches MSPs and Consultants how to implement and maintain a Cybersecurity Compliance Program
- 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"**
- Co-Star and Co-Producer of documentary **"Cybercrime: The Dark Web Uncovered"**
- Author of 2 Books:
  - **"Cyber Warfare: Protecting Your Business From Total Annihilation"**
  - **"The 3 Indisputable Rules Every Manufacturer Must Know Before Purchasing Any IT Product or Service"**

CISM

CAICO CERTIFIED CMMC PROFESSIONAL

CYBER AB REGISTERED PRACTITIONER ORGANIZATION RPO



CompliancyIT

DISCLAIMER:

CMMC is a new DoD Program.

As a new Program, there are things that sound good on paper, that don’t work so good in real life.

There is no way to account for all questions or scenarios that can be encountered before a new Program is stood up and implemented.

There will continue to be clarification and normalization of how situations are handled as the Program is developed.

CompliancyIT

Assessors WANT You To Pass!

- Not the enemy
- They WANT you to be successful
- …but you need to meet them with the information they need
- So, what do you need to have?

CompliancyIT

A Solid System Security Plan (SSP)

- Describes the boundary clearly
- Proper statements explaining each Control AND Assessment Objective
- Acts as the “Rosetta Stone” between the controls and your company
  - NIST has its own language. Don’t change your company language to NIST, translate it
    - e.g. – “processes acting on behalf of users” = “service accounts”

CompliancyIT

A Solid System Security Plan (SSP)

EXAMPLE Environment :

- M365 & Intune – SPA
- Laptops – CUI Assets
- Box – CUI Asset

AC.L2-3.1.1 – AUTHORIZED ACCESS CONTROL [CUI DATA] Limit **system access** to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]11 Determine if:

[a] authorized users are **identified**;

[b] processes acting on behalf of authorized users are **identified**;

[c] devices (and other systems) authorized to connect to the system are **identified**;

[d] system access is **limited** to authorized users;

[e] system access is **limited** to processes acting on behalf of authorized users; and

[f] system access is **limited** to authorized devices (including other systems).

NOT GOOD:

- We identify authorized users and assure that the system is limited to authorized users. We identify processes active on behalf of authorized users assure that the system is limited to processes acting on behalf of users. We identify devices connected to the system and assure that the system is limited to authorized devices.

GOOD:

- Authorized users, processes acting on behalf of authorized users (service accounts), and devices authorized to access the M365 and Box systems are identified on the **Asset Management Plan**. The AMP is reviewed quarterly to assure it correctly reflects authorized users, service accounts, and devices and is compared to the environment. After the quarterly review, any unauthorized users, service accounts, or devices are removed from M365 and/or Box environments. Authorization for new users, devices, and service accounts can be requested by Technology Decision Makers and their approval follows the **change management process.**

CompliancyIT

A Solid System Security Plan (SSP)

EXAMPLE Environment:

- Vulnerability Scanner – Qualys
- M365 – CRMA
- On Prem AD Server and endpoints

RA.L2-3.11.2 – VULNERABILITY SCAN

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]174

Determine if:

[a] the **frequency** to scan for vulnerabilities in organizational systems and applications is defined;

[b] vulnerability scans are performed on **organizational systems** with the **defined frequency**;

[c] vulnerability scans are performed on **applications** with the defined frequency;

[d] vulnerability scans are performed on organizational systems when **new vulnerabilities are identified**; and

[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

NOT GOOD: (restate the AO's)

- The f**requency** to scan for vulnerabilities in organizational systems and applications is quarterly. Vulnerability scans are performed on **organizational systems** quarterly. Vulnerability scans are performed on **applications** quarterly. Accountability for this process is achieved by providing reports for analysis. Vulnerability scans are performed on organizational systems when **new vulnerabilities are identified** and vulnerability scans are performed on applications when new vulnerabilities are identified.

GOOD: (tell the story)

- Qualys is used to scan for vulnerabilities quarterly, as defined in the **IT Security Policies**. Scans are run on both the in scope information systems (on premises servers and computers as well as M365) and is also run against the applications (see **Approved Software List**). The scans are reviewed before and at the **Quarterly Risk Management Meeting** as a mechanism of accountability for this process. When we are alerted to new vulnerabilities from CVE feeds or vendors, per the **Security Alerts and Advisories SOP**, a scan is run within 7 days to assess whether the vulnerability pertains to the information system or installed applications.

CompliancyIT

A Clarified Scope

- Network Diagram
  - Detailed to assure the internal and external boundaries and asset relation to each other is clear
- Data Flow Diagram
  - How FCI and CUI is flowing throughout the business process
- CMMC Assets Diagram
  - Shows how you categorized the assets in scope to assure your categorization matches the assessor’s

CompliancyIT

Documentation REALLY Matters

- What's on paper really matters – NO CYA
- "Values" or Organizationally Defined Parameters (ODPs) in documentation must match real life
- Show versions, policies must be signed
- If you have a process for something (IT process, data handling process, physical protection process) there must be a corresponding written document for it

CompliancyIT

Things That May Be A “Gotcha”

- Documentation of Ports, Protocols, and Services
  - Permitted per devices or device type
  - Means that you have to disable or remove those that are not permitted
  - Everything cannot be permitted (Xbox anyone?)
  - Can be in the form of lists or detailed in a baseline configuration
  - Must demonstrate this is controlled

CompliancyIT

“Essential Software”

- Approved Software List
  - What’s allowed on computers, servers, other devices, by device type and/or by department or role
  - Remove any software that is not approved/on the list
  - Include Enterprise Apps in M365

CompliancyIT

“External Connections”

- What external information systems are permitted?
  - External Information System = an information system that is *external* to the compliance boundary
  - Connect to it to pass data back and forth, but you don’t control it, must accept the risk of connecting to these systems
    - DoD Safe
    - Customer web portals

CompliancyIT

Make Sure You're Doing RA and CA

- Regular Risk Assessment – document how often, show evidence you're doing it with that frequency
- Have a Risk Register, and update it
  - Utilize it as your "Operational Plan of Action"
- At least **Yearly** Security Assessment – must show documentation that you completed this process

CompliancyIT

The Importance of Evidence

- Screenshots, screenshots, screenshots
- Documentation as Evidence
  - Meeting notes/agendas
  - Training evidence
  - IT Tickets – following the documented processes
- Hashing Tool & Storing your evidence for 7 years

CompliancyIT

Know Your $h!t. Advocate For Yourself.

- Identify who assessors will interview in advance
- Must understand the processes they are being interviewed about and how they relate to the controls
- Prep the team with test questions
  - How assessors ask questions
- There are many ways to implement the controls, have a deep understanding of what control implementation looks like, and be prepared to defend your control implementation

CompliancyIT

Sum It Up

- Expect rigor
- Get your documentation aligned
- Prep your people
- Show continuous processes and evidence of your program

CompliancyIT

THANK YOU
for coming today!

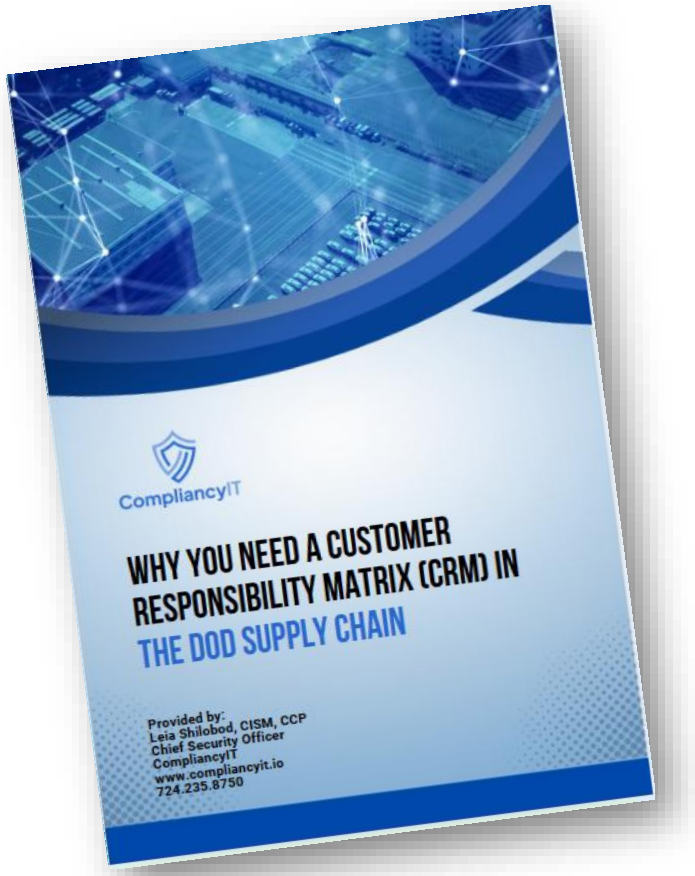
To help you with more information about what a Customer Responsibility Matrix (CRM) should look like, we'd like to send you a copy of our Free Report:

"Why You Need A Customer Responsibility Matrix (CRM) in the DoD Supply Chain"

Email "CRM"

to

Info@compliancyit.io



QUESTIONS?

“The CMMC Certification Assessment: A Behind The Scenes Look”

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