CyberCertify.me

A SERVICE OF CYBER SECURITY TRAINING AND CONSULTING LLC

CMMC CONTROL MAPPING GUIDE

SUPPORT
Info@CyberCertify.me

MAPPING CYBERCERTIFY.ME CMMC COURSES TO CMMC PRACTICES

INTRODUCTION

This CyberCertify.Me CMMC Control Mapping Guide provides information on how **we** have mapped the content of each course to CMMC requirements.

The Cybersecurity Maturity Model Certification (CMMC) is designed to help drive organizational resilience against cyber attacks.

The CMMC places requirements upon organizations that a part of the federal, and in this case the Department of Defense (DoD), supply chain. These defense industrial base (DIB) contractors are required to meet specific maturity levels in order to win DoD contracts.

The CMMC model outlines five (5) maturity levels, each with a corresponding set of processes, capabilities, and practices, which are segmented into seventeen (17) domains.

The training within our CMMC Series are designed to help organizations increase their security awareness and support certification requirements for differing maturity levels.

CONTROLS VS PRACTICES

Information security professionals familiar with national and international standards are familiar with the detailed activities organizations must perform to be compliant. The CMMC has these same requirements but they are referred to as practices. Although the capabilities and processes within the CMMC are important, and required, they are overarching and higher level. As a result, when you see practices, think controls.

CMMC DOMAINS

The 17 CMMC domains are noted below as reference before we discuss mapping.

- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communications Protection (SE)
- System and Information Integrity (SI)

MAPPING APPROACH

A cornerstone philosophy of Cyber Security Training and Consulting LLC is that in order to transform humans from the weakest link in the security chain into the strongest requires a broader understanding of the complex online threat environment.

As a result, we often include related topics across multiple courses. This ensures foundational topics are addressed. Therefore, when you view the mappings below, you will see mappings that may not inherently be obvious based on the course topic or learning objective.

Is this overkill and needless? Hardly. Although the CMMC is a compliance framework, the intent is to secure organizations and personnel and we are confident our approach truly addresses this.

That said, we're human too so mistakes can be made. We strive for perfection but because Certified CMMC Assessors are humans with opinions, we may not meet the mark for a given assessor. If this happens, just let us know. We can typically fix issues in 24 hours or less so your assessment isn't held up due to an inferred weakness in our content.

MAPPINGS

Below are our CMMC courses, the learning objectives of each course, the CMMC maturity level(s) targeted by the course, and the CMMC practices we map the content to. However, keep in mind that even though we may target a specific level it doesn't mean the content is only valuable to organizations at the given maturity level; all of our content is valuable to an organization at every level.

- ## ADVANCED PERSISITENT THREATS (APTS)

Learning Objectives:

- The different types of hackers
- The main categories of hackers
- The motivations of advanced persistent threats and the impact they can have on organizations

Target CMMC Level(s):

- Level 4 - 5

CMMC Practice(s) Supported:

- AT.4.059: Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

- ## BREACHES

Learning Objectives:

- What a data breach is and the impacts to organizations
- Which countries are targeted most and the success of attacks
- What happens to stolen data and how it is used

Target CMMC Level(s):

- Level 4 - 5

CMMC Practice(s) Supported:

- AT.4.059: Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

- ## INSIDER THREATS

Learning Objectives:

- What an insider threat is
- Common signs of insider threats
- Steps to take to mitigate insider threat risk

Target CMMC Level(s):

- Level 3 - 5

CMMC Practice(s) Supported:

- AT.3.058: Provide security awareness training on recognizing and reporting potential indicators of insider threat.

- ## NEW EMPLOYEE ONBOARDING (MANAGEMENT & STAFF VERSIONS)

Learning Objectives:

- Teamwork: How high-performing teams are able to function
- Roles: The importance of each employee knowing their role
- Responsibilities: How organizations and employees are reliant on clearly defined responsibilities

Target CMMC Level(s):

- Level 2 - 5

CMMC Practice(s) Supported:

- AT.2.056: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

• POLICIES, STANDARDS, AND PROCEDURES (MANAGEMENT & STAFF VERSIONS)

Learning Objectives:

- What a policy is, its purpose, value, and examples of common information security policies
- What a standard is, its purpose and its relationship to a policy and procedure
- What a procedure is, its purpose, and how it relates to a policy and standard
- How policies, standards, and procedures are related in an overarching framework

Target CMMC Level(s):

- Level 1 - 5

CMMC Practice(s) Supported:

- AC.1.003: Verify and control/limit connections to and use of external information systems.
- AC.1.004: Control information posted or processed on publicly accessible information systems.
- AC.2.006: Limit use of portable storage devices on external systems.
- AC.2.016: Control the flow of CUI in accordance with approved authorizations.
- AT.2.056: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- MA.3.115: Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- MP.1.118: Sanitize or destroy information system media containing Federal Contract information before disposal or release for reuse.
- MP.2.119: Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- MP.3.122: Mark media with necessary CUI markings and distribution limitations.
- MP.3.123: Prohibit the use of portable storage devices when such devices have no identifiable owner.
- PE.1.131: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- PE.1.132: Escort visitors and monitor visitor activity.
- PE.1.133: Maintain audit logs of physical access.
- PE.3.136: Enforce safeguarding measures for CUI at alternate work sites.
- SC.3.193: Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).

MAPPING CYBERCERTIFY.ME CMMC COURSES TO CMMC PRACTICES

SECURITY RISKS

Learning Objectives:

- Threat Agents: Examples of cyber threat agents far and near
- Organizational Cyber Risks: The top cyber risks facing organizations
- Employee Cyber Risks: The top cyber risks facing employees
- Cyber Attack Response: What employees should do when a victim of a cyber attack

Target CMMC Level(s):

- Level 2 - 5

CMMC Practice(s) Supported:

- AT.2.056: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

SOCIAL ENGINEERING

Learning Objectives:

- Threat Agents: Examples of cyber threat agents far and near
- Organizational Cyber Risks: The top cyber risks facing organizations
- Employee Cyber Risks: The top cyber risks facing employees
- Cyber Attack Response: What employees should do when a victim of a cyber attack

Target CMMC Level(s):

- Level 4 - 5

CMMC Practice(s) Supported:

- AT.4.059: Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

SUSPICIOUS BEHAVIOR

Learning Objectives:

- The most common types of suspicious behavior
- What to look for in order to identify suspicious behavior
- Whose responsibility it is to report suspicious behavior

Target CMMC Level(s):

- Level 4 - 5

CMMC Practice(s) Supported:

- AT.4.059: Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

OH, SNAP!

We hope you find value in our training. We really have worked hard to make the training more informative, more consumable, more valuable, and more interesting. But, like we said before, we are humans and prone to mistakes.

If you find any of the following issues with our training, let us know, and if it hasn't already been identified, we'll send you a complimentary t-shirt. It's our way of saying sorry and thanks.

- Typos
- Factually incorrect content
- System or site data or functional issues
- Blatant grammatical faux pas
    - Note: Wordsmithing (e.g., you'd say something differently, doesn't qualify)

CLOSING

Thanks again for being a customer. We are proud to be a CMMC-AB Licensed Training Provider (LTP) and an active member of the CMMC ecosystem. Securing the federal supply chain is imperative and we sincerely strive to support this mission.

As you may already know, the CMMC courses are quite targeted to align to the CMMC, however, increasing security awareness is best served through regular and broad employee awareness. When it comes to security awareness training, "Set it and forget it" is a terrible idea. With that in mind, we have developed the incredibly affordable 60 Seconds of Cyber micro-series of courses that include a variety of short (less than 3 minutes each) courses on various security fundamentals topics, hacker groups, and hacker profiles. We encourage you to consider adding these to your arsensal.

Finally, we want to hear from you! Want to shower us with praise? We'll take it! Do you have an idea on how we can elevate our game? That's cool, we can take constructive criticism. Want to hate on us? Bring it on! We know how to make lemonade. Send it all to: info@cybersecuritytrainingco.com.

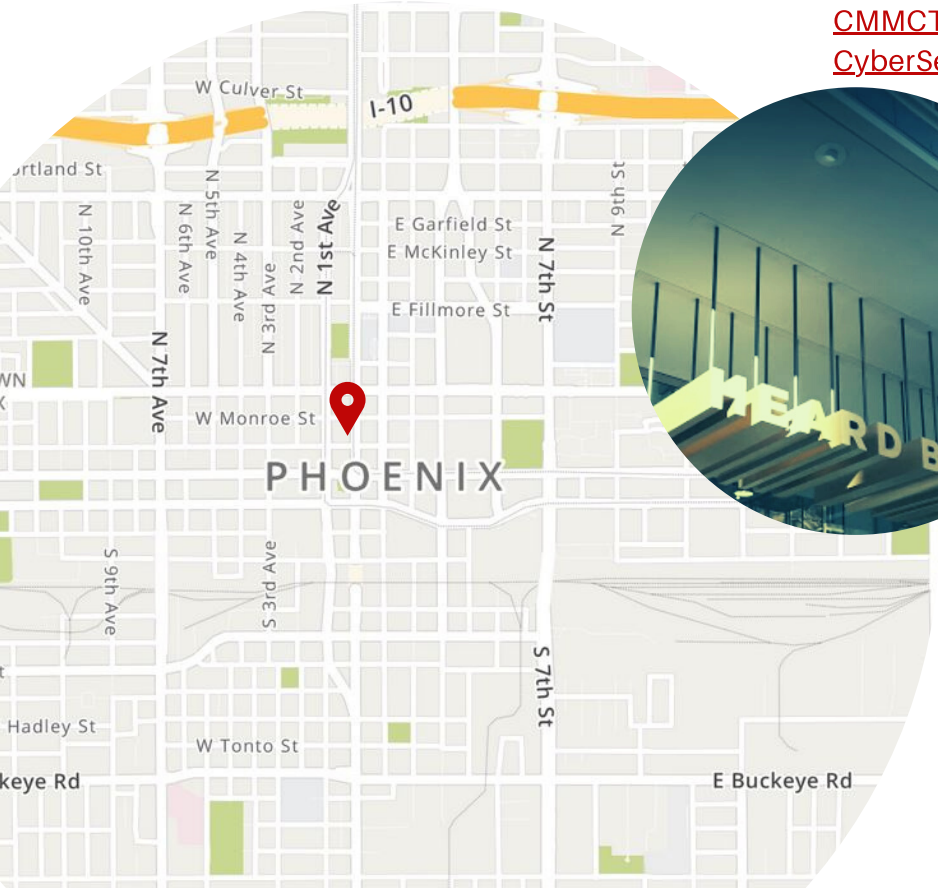
CyberCertify.me

CYBER SECURITY TRAINING AND CONSULTING LLC

CONTACT US FOR HELP

We've tried to cover all the bases in this user guide but it's possible we missed something! Our apologies if this happens. Please contact us if you have any questions, need some help with CyberCertify platform, or experienced an error (Yikes!).

CYBER SECURITY TRAINING AND CONSULTING LLC
112 North Central Avenue
Suite M09
Phoenix, AZ 85004
CyberCertify.me
CyberCrisisResponse.com
CMMCTraining.Academy
CyberSecurityTrainingCo.com



North/West Bound
Stop #10032
Washington/Central

South/East Bound
Stop #10013
Jeffrerson/1st Avenue