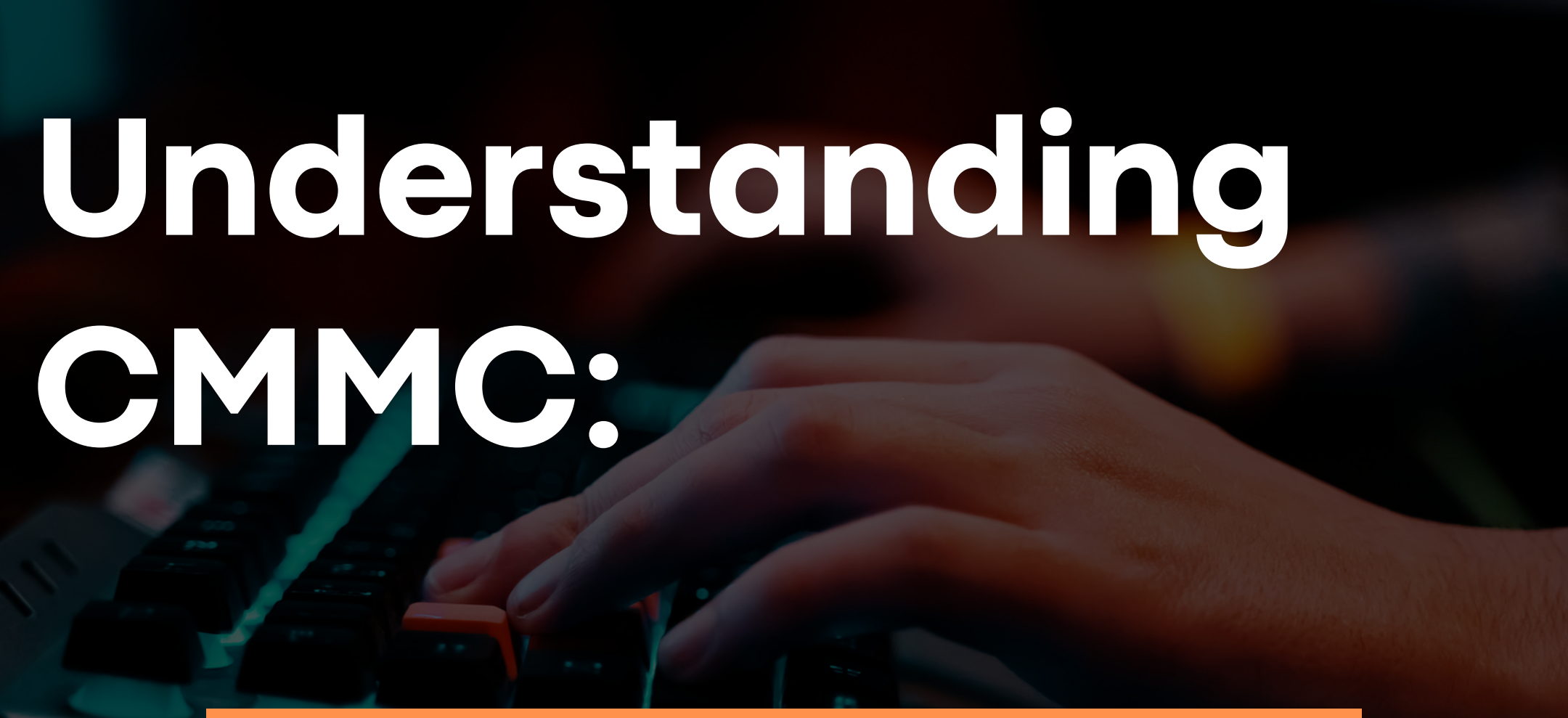
CYNEXLINK
YOUR BUSINESS FIRST

A How-to-Guide to Become CMMC Compliant

***A pre-requisite to retain your DoD supply chain contracts!**



Understanding CMMC:

The CMMC framework includes a set of processes, controls, and practices that defense contractors must implement to protect controlled unclassified information (CUI) and federal contract information (FCI).

The framework consists of 3 levels, each representing an increasing level of maturity in cybersecurity practices, with Level 1 being the most basic and Level 3 being the most advanced.

To bid on DoD contracts, defense contractors must be certified at the appropriate CMMC level for the contract they are seeking.

Compliance Requirements & Levels :

CMMC compliance refers to the state of adhering to the requirements and controls outlined in the Cybersecurity Maturity Model Certification (CMMC) framework.
The CMMC compliance requirements vary depending on the level of certification sought by a contractor. For example:

1 **CMMC Level 1 (Foundational):**

17 Practices; it is the most basic level of CMMC compliance, requiring basic cybersecurity practices such as antivirus software and background checks and only Annual self-assessment.

2 **CMMC Level 2 (Advanced):**

110 practices aligned with NIST SP 800-171; requires additional security controls like employee training and incident response planning and Triannual third-party assessments for critical NSI.

3 **CMMC Level 3 (Expert):**

110+ practices based on NIST SP 800-172; it requires further controls like network access limitations, vulnerability assessments and Triannual government-led assessments.

What Steps you Need to Take to Become a Compliant:

1 ASSESSMENT AND GAP ANALYSIS:

You need to get a comprehensive assessment of your organization's current security posture and identify any gaps or weaknesses in the security controls. This will help your organization understand what areas needs to improve to meet CMMC compliance requirements.

2 SECURITY SOLUTIONS:

You need to implement various security solutions to help your organization meet the CMMC compliance requirements. For example, you need a solution that can provide endpoint protection, network security, and data encryption solutions.

3 TRAINING AND EDUCATION:

Your organization needs training and education on CMMC compliance requirements and how to implement the necessary security controls.

4 THIRD-PARTY AUDITOR:

Your organization needs a third-party auditor for CMMC compliance. They will evaluate your company's implementation of the required controls and practices to determine whether they meet the CMMC level sought. Their assessment results will be submitted to the CMMC Accreditation Body for final certification approval.

Cynexlink can play a significant role in helping your organization achieve and maintain CMMC compliance by providing assessment, solutions, training, and managed services.

If you need help taking these steps, we're working with clients to implement these, and we can hop on a quick call and help assess your situation.