# CMMC Readiness Assessment

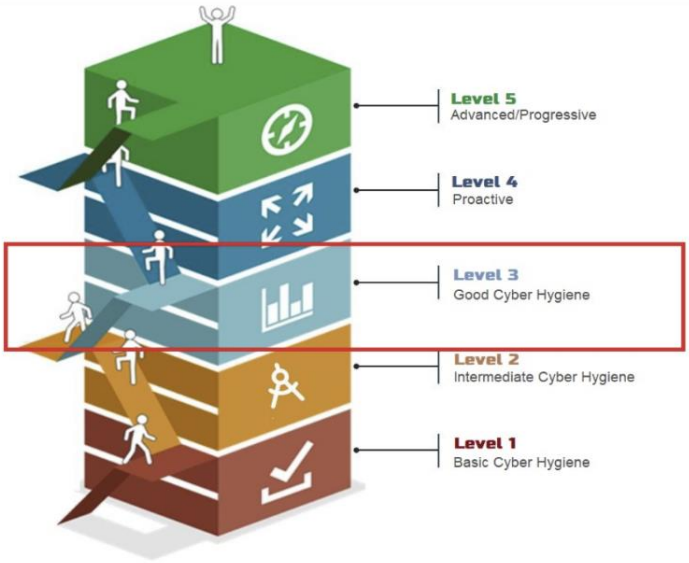
**Company: JDK Technologies**
**Data Provided By; John Smith**
Date: Sep 4th, 2020

## Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) framework consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD) stakeholders. The model measures cybersecurity maturity with five levels. Each of these levels, in turn, consists of a set of processes and practices. The CMMC framework also added a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. For contracts that require CMMC, a vendor may be disqualified from participating if the organization is not certified. The DoD will specify the required CMMC level in the RFIs and RFPs.

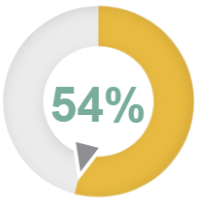
This report is based on your CMMC readiness assessment and provides a completion analysis for each of the domains. This should provide you with an idea on the effort required to have in place the remaining practices before engaging the CMMC certifying auditor.

JDK Technology's Target CMMC Maturity Level




For Level 3, you have to comply with 130 practices to get certified.

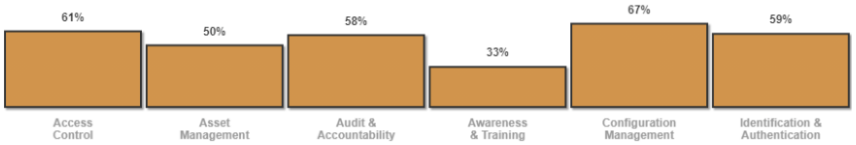
## JDK Technology's Current Progress Towards Meeting the Goal

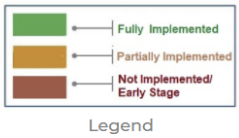


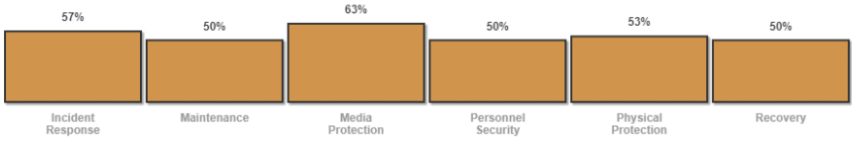

JDK Technology's progress towards completing all the pratices required for the CMMC maturity level is estimated at 54%. Before you can schedule the auditor to conduct the CMMC audit and certification, the completion score need to be at 100%. As a next step -

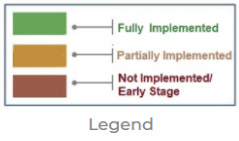
- Review your progress in the each of the domains
- Review the action plan in this report
- Obtain senior leadership sponsorship for this project
- Obtain necessary funds and resource to complete the CMMC certification and begin executing on the project tasks
- If you need help with the project tasks, Zartech can assist you with professional services

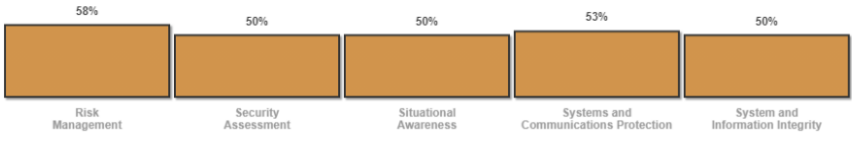
**Ballpark percentage of completion within each of the CMMC domains applicable to you:**

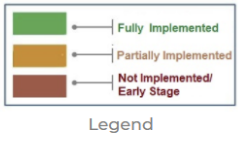


# Action Plan


**Before JDK Technology can schedule the auditor to come in to do the CMMC audit and certification, the completion score need to be at 100%. Note that receiving Cybersecurity Maturity Model Certification requires all practices and processes to be implemented at the time of certification assessment. Any security requirements that were part of a plan of action must be closed/met in order to be granted the CMMC certification.**

## CMMC Audit Preparation

**Preparing for the CMMC audit**

The first step would be to download the latest version of the CMMC here (download the appendix!). Next, based on the CMMC maturity level that you are targeting, understand all the practice requirements for that level.

**Identify the scope of your audit**

CMMC would only apply to systems that contains specific types of data, such as Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). To narrow the scope of the audit, conduct a data mapping exercise to find out where all the related data are stored, processed and transmitted. After you have identified the systems that would be within the scope of the audit, take the CMMC practice requirements and align them to each of the system(s). Create all the required Policies, Standards, and Procedures. Note that addressing the people, processes and technologies around CUI is a necessary part of any CMMC/NIST 800-171 compliance program.

**How many hours will it take to complete project tasks and evidence gathering?**

There are three factors for estimating the cost and work involved with compliance.

- How complex is the network you are evaluating?
- Does your network already have secure configurations and security programs installed?
- What CMMC level are you trying to meet?

Is it possible to isolate your information to fewer systems, fewer networks, or fewer users, while still fulfilling the terms of your contract? You don't need to secure ALL computer systems for the entire company. You just need to secure the systems that store data (Controlled Unclassified Information) about the contract. Make the job easier by reducing your footprint.

Pouring over controls and analyzing infrastructure is a tedious and time-consuming process. If you involve an experienced SME at your organization who knows your environment well, this process will take less time.

Zartech offers professional services that can help you complete the compliace requirements, such as -

- Custom policy, standards and procedures development
- Penetration testing of your application and network
- Incident response program development

Please contact us, if you need any assistance by emailing us at info@zartech.net or call us at 214-631-9353.