

WHITE PAPER

Cybersecurity Maturity Model Certification (CMMC)

Thousands of clients use NetSuite as their Enterprise Resource Planning (ERP) system of choice to manage their businesses. The Daston Corporation provides the way for U.S. Federal Government Contractors to obtain and maintain Federal Acquisition Regulation (FAR) and Cost Accounting Standards (CAS) compliance. Daston is committed to providing “NetSuite Compliance Ready Solutions” as part of our DCAA-on-Demand SuiteApp and service offerings. To provide further support to our GovCon user community, Daston is sharing our roadmap for CMMC and how we plan to help our clients prepare for these new regulations.



Cybersecurity Maturity Model Certification (CMMC)

Table of Contents

- Overview of CMMC
- Entities Impacted by CMMC
- CMMC Requirements as of 2024
- Conclusion

Introduction

In today's digital age, cybersecurity is paramount. As threats evolve and become more sophisticated, organizations must adapt to protect their sensitive information and infrastructure. The Cybersecurity Maturity Model Certification (CMMC) is a framework designed to enhance the cybersecurity posture of the defense industrial base (DIB) sector. This whitepaper aims to provide a comprehensive understanding of CMMC, its impact, and the requirements as of 2024.

Overview of CMMC

CMMC is a set of cybersecurity standards developed by the United States Department of Defense (DoD) to ensure that contractors and subcontractors within the DIB sector implement adequate cybersecurity practices. The model consists of five maturity levels, ranging from "Basic Cyber Hygiene" to "Advanced/Progressive." Each level builds upon the previous one, with increasing rigor in cybersecurity practices and controls.

The primary objectives of CMMC include:

- Strengthening the cybersecurity posture of the DIB sector
- Safeguarding sensitive information and controlled unclassified information (CUI)
- Enhancing the resilience of defense supply chains against cyber threats

CMMC incorporates various cybersecurity standards and best practices, including but not limited to NIST Special Publication 800-171, NIST Cybersecurity Framework (CSF), and ISO/IEC 27001.

Entities Impacted by CMMC

CMMC requirements affect all organizations and individuals within the DIB sector who handle sensitive information or provide products and services to the DoD. This includes prime contractors, subcontractors, suppliers, and vendors. Any entity seeking to do business with the DoD must adhere to the appropriate CMMC level based on the sensitivity and nature of the information they handle.

The rollout of CMMC requirements occurs in phases, with different deadlines for compliance based on contract requirements. By 2024, all DoD contracts are expected to include specific CMMC requirements, making compliance mandatory for organizations operating within the DIB sector.

CMMC Requirements

CMMC framework includes the following key requirements:

CMMC utilizes a tiered structure, with each level representing a growing degree of cybersecurity maturity. The specific requirements for each level are outlined in the **CMMC Accreditation Body (CMMC-AB)** CMMC 2.0 is the current iteration of the framework.

Here's a brief overview of the CMMC levels:

- Level 1: Foundational - This level focuses on basic cybersecurity practices like device and access controls.
- Level 2: Advanced - Level 2 builds on Level 1 and requires implementation of a wider range of security controls, including incident response and system monitoring. This is the likely requirement for most DoD contracts that involve CUI but don't deal with particularly sensitive information.
- Level 3: Expert - This is the highest level and is intended for organizations handling highly sensitive national security information. It demands a sophisticated cybersecurity posture with robust processes and procedures.
-

The specific requirements for each level are outlined in the **CMMC Accreditation Body (CMMC-AB)**

Conclusion

CMMC represents a significant step forward in enhancing the cybersecurity resilience of the DIB sector. By establishing a tiered maturity model, CMMC provides organizations with a roadmap for improving their cybersecurity posture over time. Compliance with CMMC requirements is mandatory for all government contractors seeking to do business with the DoD. By adhering to the appropriate CMMC level and implementing robust cybersecurity practices, organizations can better protect sensitive information and contribute to the overall security of the defense supply chain.

As many of Daston's clients are aware, we are also a Federal Government Contractor and are deeply committed to helping our fellow contractors obtain and maintain compliance. Daston is firmly established to assist you to navigate CMMC requirements for your accounting and financial solutions. Reach out to our experts today!



ORACLE
NETSUITE
Solution Provider

ORACLE
NETSUITE
SuiteCloud Developer Network



JOE ALSTON
VICE PRESIDENT OF SALES

Email: joe.alston@daston.com
Phone: 703-249-9682