



# Cybersecurity Maturity Model Certification (CMMC)

## CMMC Gap Analysis

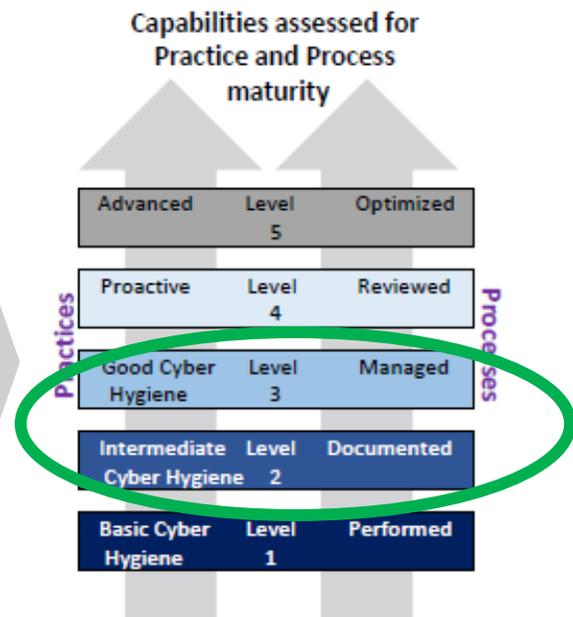
Cyber attackers are exposing all kinds of weaknesses in your best defenses. As attacks become increasingly sophisticated, it's more important than ever to identify and mitigate those weaknesses before they get hacked; and build a company culture that makes cybersecurity a priority.

The Michigan Economic Development Corporation's (MEDC) Michigan Defense Center (MDC) has identified Michigan contractors to provide cybersecurity compliance consulting services for small and medium-sized Michigan businesses to assist in achieving National Institute of Standards and Technology (NIST) 800-171 compliance and relevant DFARS requirements in order to qualify for United States Departments of Defense (DoD) and Homeland Security (DHS) contracts and work in the federal supply chain.

COLT CSC, a pre-qualified contractor, conducts a Gap Analysis to identify and quantify security vulnerabilities in your IT environment. Our security experts evaluate weaknesses that attackers will target, and provide mitigation options to eliminate or reduce your risk.

The **COLT CSC CMMC Gap Analysis** covers: **14 DOMAINS**

Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)
Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)
Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)
Physical Protection (PE)	Risk Management (RM)	Security Assessment (CA)
System & Communications Protection (SC)	System & Information Integrity (SI)	



## Is CMMC Gap Analysis right for you?

Your security solution should evolve with the changing threats, but many IT departments are being asked to do more with less and may not have the time or resources to perform a proper vulnerability assessment. Equally important is that many organizations may be required to conduct these assessments in order to meet regulatory compliance standards.

## A CMMC Gap Analysis from COLT CSC, helps your business:

- Develop a roadmap towards CMMC Level 3 compliance
- Identify higher-risk vulnerabilities
- Provide justification for increasing security investment or validating current strategy
- Determine SPRS Compliance requirements
- Remain Competitive/Stay compliant
- Discover new set of attack vector
- Partner with cyber security experts to grow your company into tomorrow's environment

## Methodology

Your company receives an on-premise, virtual or hybrid assessment. Our experts work alongside your company's IT staff to guide and mentor the 110 NIST security controls. It all begins with a one-hour kick-off meeting that includes the senior leadership team to set conditions that cybersecurity is an environment, or corporate culture, rather than a checklist.

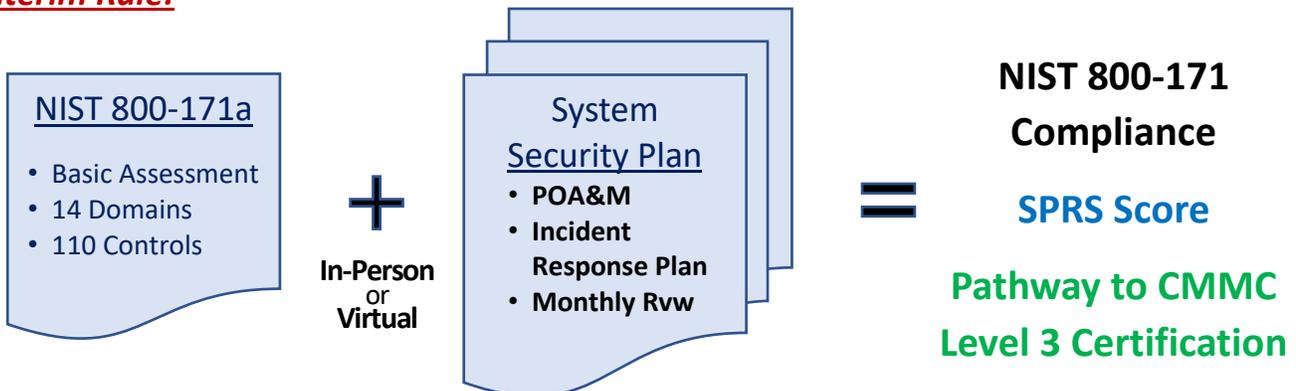
Your company is assessed using one, two or all three methods of examination, testing and interview to obtain a body of evidence. A comprehensive report breaks-down the 14 DOMAINS and scores overall compliance against NIST 800-171 security controls. The security controls not meeting NIST compliance are consolidated and organized into a prioritized list to help IT staffs determine which practices to remediate in order of precedence or level of vulnerability. Additionally, the assessment team determines the company's Supplier Performance Risk System (SPRS) score and assists the company's input of the SPRS into the federal database.

COLT CSC has the expertise to manage each of the NIST security controls. This allows companies to partner with COLT CSC subsequent a CMMC Gap Analysis to strengthen the cybersecurity posture. Using a Good, Better, or Best format, COLT CSC enables companies to evaluate remediation options for cost and effect.

## Why COLT CSC?

Our team of expert security professionals have assisted federal and state agencies across multiple industries keep networks safe in the face of growing threats. We're proud to offer the latest security solutions backed by a team with broad certifications, unique experiences and expertise. Our team will improve your business and its security posture; while freeing up those you need to focus on the initiatives that help grow revenue.

### Interim Rule:



Contact: **COLT Cyber Security Consultants**

616.581.3894 / [mtellier@coltcsc.com](mailto:mtellier@coltcsc.com)