



PREPARATION GUIDE

Cybersecurity Maturity
Model Certification



CMMC PREPARATION GUIDE

Mature Your Cybersecurity Systems.
Prepare for the CMMC.

In November 2021, the Department of Defense (DoD) announced the strategic direction of the Cybersecurity Maturity Model Certification (CMMC) program moving forward, as well as the launch of CMMC version 2.0. This new version of the cybersecurity framework for the Defense Industrial Base (DIB) simplifies the standards, provides additional clarity, and streamlines the assessment requirements. **Per current guidance, CMMC compliance will become a requirement of civilian and defense contracts by the summer of 2023.**

For the over 300,000 companies in the DIB, meeting, at a minimum, Level 1 accreditation requirements by passing a CMMC security assessment will be critical to doing business with DoD.



CMMC 2.0 AT A GLANCE



Three
maturity
levels



110+
cybersecurity
best practices

Assessments



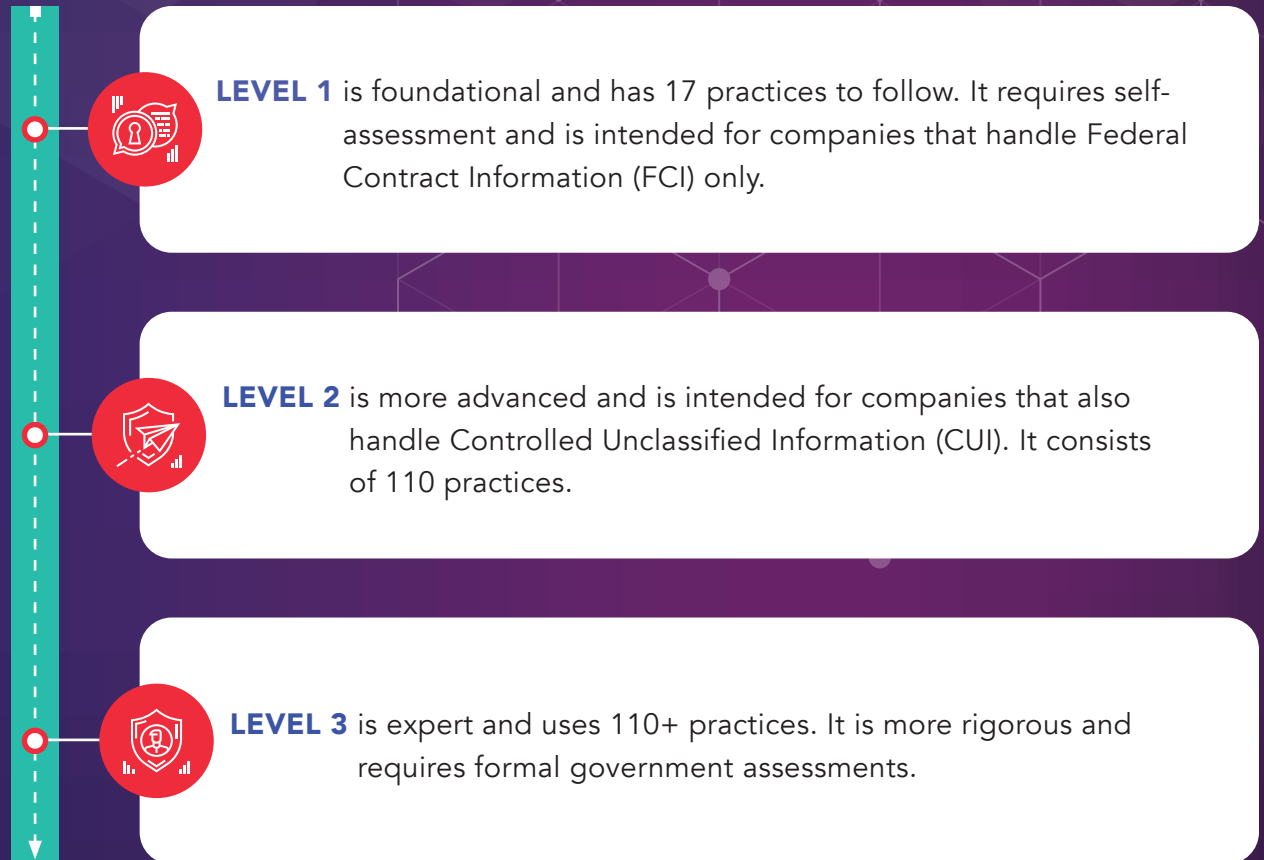
All companies
in the DIB
must complete
a CMMC
assessment

CMMC PREPARATION GUIDE

Model Overview

CMMC consists of three maturity levels including 110+ practices, which progress from basic cyber hygiene to advanced cyber defense. Companies can scope the certification for the entire organization or for specific business segments or enclaves. Although CMMC accreditation is not required at the time of bidding, it must be in place by the time of the contract award.

Level 1 begins with the basic safeguarding of federal contract information (FCI), introducing heightened security controls to protect controlled unclassified information (CUI) in level 2. Level 3 bolsters CUI protection through enhanced security requirements.



CMMC PREPARATION GUIDE

The CMMC Process



Pre-Assessment

Begin reviewing your company's alignment to CMMC as early as possible before a new contract anticipated start date.

After identifying your desired CMMC Maturity Level and scope, conduct a pre-assessment to identify and close any gaps before your official CMMC Assessment.



Undergoing Assessment

Search the Cyber Accreditation Body's (The Cyber-AB) marketplace to find a certified third-party assessor organization (C3PAO) to conduct your assessment.

Work with your C3PAO to schedule and conduct the CMMC assessment, which will then be reviewed by The Cyber-AB.



Post-Assessment

If any unsatisfied practices are uncovered during your assessment, your company will need to track the remediation in a Plan of Actions & Milestones (POA&M).

By working with a company like ECS to prepare for the CMMC assessment, your organization can eliminate this step by resolving any security gaps before the assessment takes place.

Your CMMC certification will be valid for three years, allowing your organization to receive DoD contracts up to the issued maturity level.

CMMC PREPARATION GUIDE

The ECS Solution



With the dedicated resources of our Cyber Center of Excellence, as well as over 20 years of experience delivering risk mitigation and compliance solutions, ECS does more than prepare your company to pass an assessment. Our experts work closely with your team to integrate better, smarter security controls in your existing information security program — leaving your company stronger, better positioned, and more secure.

- *Custom-tailored solutions to meet your company's specific needs, anticipating and solving challenges and pain points before they threaten to disrupt your business.*
- *Technical SMEs work hand-in-hand with your CISO, business unit leads, and other executives to implement missing technologies, capabilities, and practices.*
- *Compliance SMEs write SOPs and create all necessary documentation to verify compliance with CMMC.*
- *Communicate early and often to facilitate organizational change, including step-by-step guides to new practices/technologies and clear paths for employee support.*

CMMC PREPARATION GUIDE

Key Components of the ECS Solution



Preparedness Evaluation

Our expert personnel analyze the people, processes, and technology of your company's cybersecurity program to ascertain how they align with the practices of the CMMC.



Compliance Consultation

After a preparedness evaluation, ECS works with you to identify what controls your company should implement to reach your ideal certification level.



Assurance Support

We help you establish a remediation roadmap — including plans of action and milestones (POA&M) — to mitigate risks and ineffective controls.





Documentation

We work with you to document strategies, standards, and policies to meet the requirements of the CMMC and enhance your cybersecurity practices.

CMMC PREPARATION GUIDE

Solutions/Technology Areas by CMMC level

Our experts leverage ECS' proven policies, processes, and procedures with the latest technologies to raise your cybersecurity posture. Through our managed service offering, we integrate these toolsets and capabilities into your existing systems.

LEVEL 1	LEVEL 2		Additional Cybersecurity Best Practices	
<ul style="list-style-type: none"> NGAV EDR Application Management Account Monitoring Media Sanitization 	<ul style="list-style-type: none"> SIEM Vulnerability Management Removable Media Device Control Privileged Account Management Backups Encryption SOAR Threat Intelligence Platform Mobile Device Security Security Awareness Training 	<ul style="list-style-type: none"> Multi-Factor Authentication Data Classification Data Loss Prevention Wireless Access Point Security (AC.3.012) Firewall (SC.3.183) Zero-Trust Network Access (SC.3.184) CASB (SC.3.193) Email Security 	<ul style="list-style-type: none"> NAC Security Awareness – Additional Focused Areas Threat Intelligence Data Feeds Threat Intelligence Platform Penetration Testing Third-Party Cyber Risk Management Web Gateway Sandboxing Systems Component Discovery and Inventory (e.g., firmware level, OS type) (AM.4.226) 	<ul style="list-style-type: none"> Deception Application Whitelisting (CM.4.073) Security Operations Center (IR.4.101) Rogue Network Device Identification (Wireless Access Point AC.5.024) Data Integrity Digital Forensics Cyber Incident Response Team Packet Collection & Storage UEBA
				
<p>Here at ECS, we have provided risk mitigation and compliance as a service to customers for over 20 years. Our expert personnel are ready to help your company ace the assessment and navigate CMMC 2.0 compliance.</p>				
				
<p style="text-align: center;">SHAYLA TREADWELL Vice President, Governance, Risk, and Compliance</p>				

CMMC PREPARATION GUIDE

If your company does business with DoD, you can't afford to ignore the cybersecurity guidance stipulated by CMMC. Not only will a CMMC certification soon be a requirement of all DoD contracts, and likely many civilian contracts as well, but adopting the practices and processes within will help keep your company—and our nation—safe.

Let ECS help mature your company's cybersecurity posture. Our experts will guide you through the CMMC process, from initial evaluation through passing the final assessment.

Reach out and speak to an expert today at cyber@ECStech.com

Glossary

C3PAO

Certified Third-Party Assessor Organization

APT

Advanced Persistent Threat

CMMC

Cyber Maturity Model Certification

The Cyber AB

Cyber Accreditation Body

CUI

Controlled Unclassified Information

FCI

Federal Contract Information

 CMMIDEV /3  CMMISVC /3  ITIL  ISO 9001:2015  ISO/IEC 20000-1:2011  ISO/IEC 20243:2018  ISO/IEC 27001:2013

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams approach and solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.