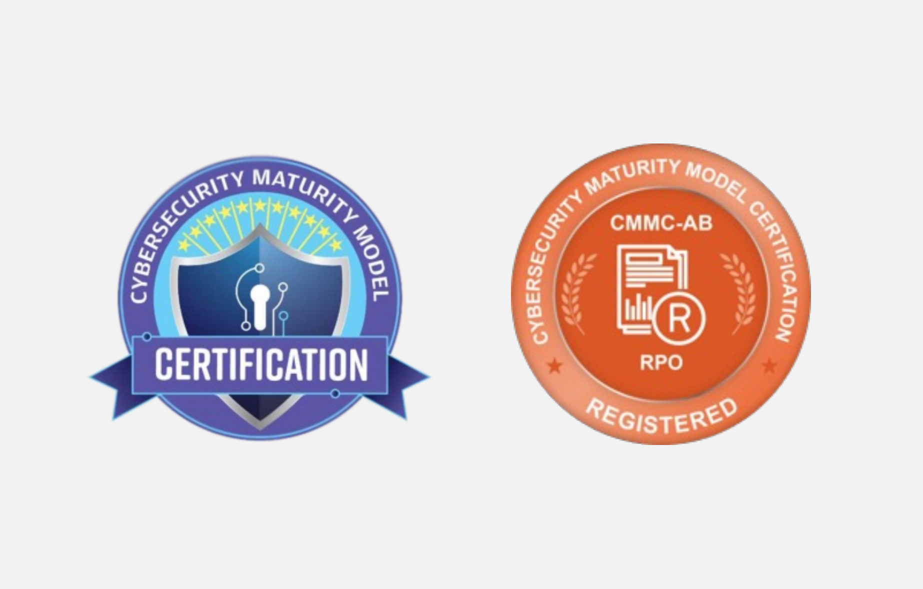
CMMC Level 2 Requirements Checklist

proarch

To create a unified security standard across the Defense Supply Chain (DSC), the Department of Defense (DoD) has implemented the Cybersecurity Maturity Model Certification (CMMC) program for all contractors.

The DoD began soliciting contracts that include CMMC requirements in FY21. If you're a contractor or sub-contractor, the time to develop a plan for remediation of security gaps and on-going compliance management is now.

There are three levels within the CMMC framework. This checklist will guide you through ProArch services that support reaching CMMC Level 2 (previously Level 3 under CMMC v1). CMMC Level 2 includes all NIST SP 800-171 controls and removes the 20 additional process requirements under version 1.


CYBERSECURITY MATURITY MODEL
CERTIFICATION
CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

Our roster of Registered Practitioners will guide you through the full journey to achieving CMMC compliance, from uncovering security gaps and remediation to on-going compliance management.

ProArch prepares your company to demonstrate maturity of implementation of CMMC requirements needed for certification.

> "Do not wait on CMMC. If you have the DFAR rule on your contract, then you are self-attesting that you are doing 110 of those controls, so do not wait."
>
> **KATIE ARRINGTON** | CISO for Assistant Secretary for Defense Acquisition

Control	Description	Required or Optional	Recommended Solutions	Complete
Virtual Chief Information Security Officer	A named CISO is not required for CMMC, but a vCISO can help drive implementation progress and keep the business informed of compliance.	Optional	• vCISO • ProArch GRC Managed Services	□
Pre-Assessment Readiness Review / POAM Development	If the organization is just beginning its journey to CMMC certification, an initial gap analysis can discover issues that need remediation. A Plan of Actions & Milestones process can be used to prepare for a CMMC assessment, but all items should be closed before entering the assessment.	Required	• Gap Analysis • ProArch GRC Managed Services	□
System Security Plan (SSP) Development	All organizations will be required to maintain an up-to-date SSP. The SSP should be reviewed and updated on at least an annual basis.	Required	• SSP Development • ProArch GRC Managed Services	□
Centralized Logging	Storing audit logs in a centralized location supports automated analysis capabilities including correlation of events across the enterprise.	Required	• Azure Sentinel • Attack Surface Reduction • Managed Detection and Response	□
Security Awareness Training	Users must undergo security awareness training on at least an annual basis.	Required	• KnowBe4 Security Awareness Training • Attack Surface Reduction	□

Control	Description	Required or Optional	Recommended Solutions	Complete
Attack Service Management / Vulnerability Management	The organization must identify and remediate system vulnerabilities in a timely manner.	Required	• Qualys Vulnerability Scanning • Managed Detection and Response	□
Incident Response Planning	Having an incident response plan and capabilities is required. The plan and procedures will need to include specifics related to Federal contracting law. Cyber insurance does not qualify as an incident response plan.	Required	• Incident Response Planning • Managed Detection and Response	□
Passive Network Monitoring	A passive monitoring solution can provide real-time telemetry and surveillance across the network to aid in the detection of cyber attacks.	Required	• SCADAfence • Datto RMM • OT Security Managed Services	□
Endpoint Detection and Response	Microsoft Defender for Endpoint secures the endpoint against attach and can aid significantly in the satisfaction of CMMC logging and vulnerability requirements.	Required	• Microsoft Defender for Endpoint • Managed Detection and Response	□
Multi-Factor Authentication	All systems that store, transmit, or process CUI must implement MFA. This includes email, workstations, servers, network equipment, and additional SaaS applications.	Required	• Microsoft Azure AD Premium • Microsoft Authenticator	□

Control	Description	Required or Optional	Recommended Solutions	Complete
System and Network Configuration Hardening	CMMC requires that security hardening baselines be applied to all systems.	Required	• System & Network Configuration Hardening	□
System Encryption	Encryption must be applied to all systems that are not protected by a physical boundary (mobile devices, laptops, flash drives, offsite backups, etc.).	Required	• Microsoft Windows BitLocker	□
Network Device Replacement	Any time encryption is being used to protect the confidentiality of CUI in transit, FIPS 140 validated cryptographic modules must be used. *(Meaning that some network equipment and encryption technologies might have to be replaced if used in a CUI environment.)*	Optional	• Barracuda Firewalls	□
Backup Hardening	CMMC introduces recoverability controls that are concerned with the ability of an attacker to compromise backup data.	Required	• Backup & Recovery Posture Check • Backup Hardening	□
Annual Risk Assessment	Organizations will need to undergo a risk assessment on at least an annual basis. Organizations can benefit from the professionalism of a risk assessment conducted by an expert risk management provider.	Required	• Risk Assessment	□

Control	Description	Required or Optional	Recommended Solutions	Complete
Application Whitelisting	Organizations must deploy application whitelisting on all servers and endpoints.	Required	• Microsoft Windows AppLocker	□
Data Classification and Data Loss Prevention	Having data classified, monitored, and automated controls in place to protect data aids in maintaining compliance, especially within in-scope environments.	Optional	• Azure Information Protection	□

Promote Healthy Cybersecurity

The purpose of CMMC is to promote healthy cybersecurity and improved process maturity of contractors across the Defense Supply Chain. By implementing CMMC requirements, you will better protect FCI/CUI, and position your company to win DoD contracts.

By developing CMMC, the DoD seeks to mitigate potential risks that could compromise the security of FCI/CUI. Your business will benefit from the implementation of CMMC practices and processes.

CMMC certification assessments are rigorous. Preparing for them may be intimidating but doesn't have to be. That's where ProArch comes in.

We know the intricacies of the certification process and how to navigate it. ProArch gets your company fully prepared for an assessment, so that you will be confident before entering an assessment that it will be successful.

Our rule is: Never enter an assessment unless you know you're going to pass!

proarch

ProArch has performed a wide range of consultative services around DFARS and CMMC including gap analysis, SSP development, vCISO, control and solution implementation, and network architecture strategy planning.

Our Registered Practitioners never let a client go into an assessment unless they know it will result in successful certification.

United States
Atlanta
New York
United Kingdom
London

India
Hyderabad
Bangalore
Pune
Singapore

CONTACT US TODAY →