

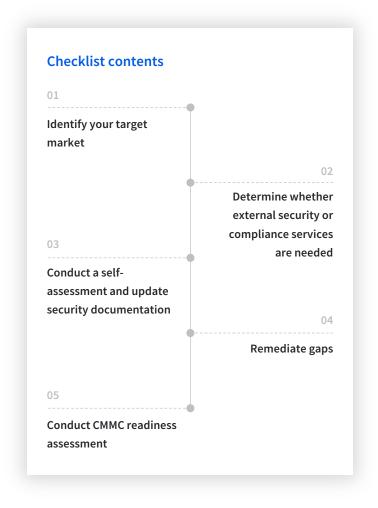
CHECKLIST

Five Steps to Cybersecurity Maturity Model Certification (CMMC) Success

AEROSPACE & DEFENSE

Contractors should begin preparing now for self-assessment and third-party certification. Successfully meeting CMMC level requirements may include investment in additional IT staff, migrating IT infrastructure, and evaluating different back office business systems, network solutions, or end user devices and software. In addition to additional resources, organizations will also need to produce and maintain extensive documentation of organizational standards, policies, and procedures as evidence of compliance.

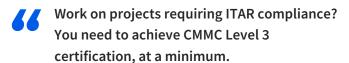
Here is a look at what operations, finance, and IT departments need to do at each step to help companies successfully run their businesses within CMMC standards.



Infor.com Five Steps to CMMC Success 1

Step 1: Identify your target maturity level

An organization's target maturity level depends on current contracts and programs you'd like to bid on in the future. Both current contractors and those new to DoD programs should review the RFIs and RFPs expected in Fall 2020 to understand what maturity levels are being required for typical program roles.



Op	perations	Notes
	Become familiar with the CMMC maturity levels	
	Determine whether current contracts and programs handle or generate Controlled Unclassified Information (CUI)	
	Understand how the company's information systems align to its operations (missions, functions, and business processes) and where CUI is stored, processed, or transmitted	
Fii	nance	
	Evaluate current and future contracts and programs for potential CMMC requirements	
	Determine timeline for when CMMC requirements will apply to the business	
	Determine impact of CMMC on near-term and long-term forecasts	
IT		
	Gather information system documentation, administrator/operator manuals, and interconnection agreements	
	Gather existing security policies, procedures, plans and any previous security assessment results (audits, vulnerability scans, physical inspections, etc.)	
	Become familiar with NIST SP 800-171 and CMMC security controls	

Step 2: Determine whether external security or compliance services are needed

Contractors need to consider the overall business impact and cost when deciding whether to pursue CMMC certification entirely inhouse or to engage external expertise and services. The quickest way to achieving CMMC certification may be to outsource some security and compliance activities to consultants or third-party IT solution vendors. The tools and skills required to achieve CMMC certification can mean a significant change in operating expenses, personnel, and administrative overhead.



Organizations that find themselves facing one or more of the following circumstances should work with qualified third-party advisors:

- · May require Level 3 or above
- Are facing NIST SP 800-171 for the first time
- · Have no dedicated security personnel

Operations	Notes
☐ Identify key resources & establish communication channels for CMMC preparation activities	
☐ Identify any gaps in internal staffing capabilities and knowledge	
☐ Estimate any additional staffing resources required	
Finance	
☐ Create business case to determine strategy for achieving certification	
☐ Develop budget to accommodate staffing and IT security requests	
IT	
☐ Identify key resources and any gaps in internal staffing knowledge	
☐ Identify critical gaps in enterprise security capabilities	
☐ Estimate any additional staffing resources and IT security tools required	

Step 3: Conduct a self-assessment and update security documentation

This step should help make the actual certification process go as efficiently as possible, providing contractors with a clear look at what security controls they need to implement, what processes they need to improve and what documentation they need to have in place to achieve certification. The self-assessment asks about security control implementation and evaluates whether the security controls are sufficiently documented, captured in policy, managed, and reviewed per each of the CMMC level requirements.

Reference the NIST Handbook 162, a selfassessment handbook for NIST SP 800-171 that uncovers baseline readiness to identify all gaps and inform development of a preliminary remediation plan for each. These plans need to be documented within a Plan of Action & Milestones (POA&M).

Op	perations
	Review the self-assessment requirements
	Identify certification team stakeholders
	Cross-reference certification requirements against current security protocols
	Document all process- and protocol-related improvement areas in POA&Ms
	If working with a consultant, serve as primary liaison for process-related improvements
IT	
	Cross-reference certification requirements against current security tools and systems
	Document all software- and infrastructure-related improvement areas in POA&Ms
	If working with a consultant, serve as primary liaison for IT-related updates

Step 4: Remediate gaps

The POA&M created in Step 3 serves as a to-do list to better organize, prioritize, and track the completion of all gap closure activities. Actions in the POA&M may require development of new organizational standards, policies, and procedures. Larger gaps may mean modifying the architecture of an organization's IT infrastructure and procurement of new software and IT security solutions.

Consider reaching out to cloud-based software providers to see how they can help. Their products may already have the security protocols in place to satisfy CMMC

requirements.

Op	perations
	Manage and monitor gap closure activities, updating documentation as you go
	Identify and lead team for development of new organizationa standards, if needed
	If working with a consultant, serve as primary liaison for process-related improvements
IT	
	Manage and monitor gap closure activities, updating documentation as you go
	Identify and lead team for security control implementation, development of new IT architecture, or deployment of new IT security tools
	If working with a consultant, serve as primary liaison for IT-related updates

Step 5: Conduct CMMC readiness assessment

After completing the previous steps, organizations are ready to repeat their CMMC self-assessment as a final readiness check before the actual C3PAO audit. Organizations that have not used external services yet may consider doing so now to raise their level of confidence. This can also serve as a practice run for the actual audit.



Repeat the self-assessment until all gaps and POA&M items have been addressed.

Op	perations
	Confirm that security awareness training has been completed by all personnel
	Confirm that all organizational standards and policies are current and readily available
	Establish continuous processes for maintaining the security program
Fii	nance
	lance
	Budget and allocate resources for continuously maintaining the security program
IT	
	Confirm that all system and security documentation are current and readily available
	Identify certification team stakeholders that will support the CMMC assessment
	Establish continuous processes for maintaining the security program

Notes		



Read the comprehensive Cybersecurity Maturity Model Certification Best Practices Guide for a look at the impact CMMC will have on defense suppliers in all tiers, as well as advice on how to turn CMMC into a competitive advantage.

DOWNLOAD NOW \longrightarrow





 $Infor \ builds \ business \ software for \ specific industries in the \ cloud. With 16,500 \ employees \ and \ over 90,000 \ customers in more than 170 \ countries, Infor software is designed for progress. To learn more, please visit \ over 100,000 \ employees \$

Copyright ©2020 Infor. All rights reserved. The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All other trademarks listed herein are the property of their respective owners, www.infor.com.

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.