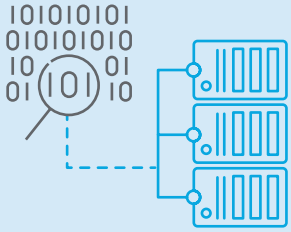
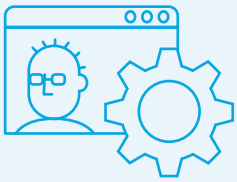
CMMC — A PRACTICAL GUIDE TO DEFINING ROLES AND RESPONSIBILITIES

Who owns CMMC compliance expectations within your organization?

Cybersecurity can seem overwhelmingly complex, but it is crucial to protecting your organization's information. Add that complexity to the pressure of the Department of Defense's (DOD) supply chain security mandate, and it's no wonder that scores of the DOD's more than 300,000 contractors lag behind in meeting the stringent requirements of the latest Cybersecurity Maturity Model Certification (CMMC) framework. In essence, the new framework poses a significant hurdle for companies seeking to provide goods and services to the DOD.

So, you're ready to square up against the CMMC and take your cybersecurity defenses up a notch. But where to begin? With decades of experience serving government contractors with cybersecurity risk management and compliance solutions, RSM has come up with a three-phase approach to navigating your CMMC compliance journey. Here's our practical guide to defining your organizational roles and responsibilities in order to properly manage your CMMC expectations.

WHAT? CMMC compliance activity	**WHO?** Functional responsibility	**WHEN?** Frequency and timing	**HOW?** Guidance and best practices on how to fulfill responsibilities
PHASE 1 — Baseline: Develop a baseline understanding of your organization's use of covered contractor information systems to process, store and transmit confidential information and controlled unclassified information (CUI).			
Contractual analysis: Identifying your contractual obligations, relationships and engagements with the DOD 	▪ Contract management ▪ Procurement ▪ Legal ▪ Sales	Quarterly	✓ Develop and maintain an inventory of existing DOD contracts that align with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and NIST SP 800-171. ✓ Include in the inventory potential contractual bids and renewals that may require future CMMC compliance.
Supply chain analysis: Identifying your vendors and subcontractors that help you administer various DOD programs	▪ Contract management ▪ Procurement ▪ Vendor management	Monthly	✓ Identify key contractors and vendors that assist you with executing your DOD programs. ✓ Become familiar with the type and flow of CUI each contractor shares with or receives from your organization.
Data identification: Developing an understanding of the type of CUI processed, stored and transmitted within your organization's environment 	▪ System media managers ▪ Data owners ▪ Data custodians ▪ Information security	Annually	✓ Develop a detailed diagram demonstrating the data flow between the corresponding applications, supporting systems and databases (internal and external) that handle CUI. ✓ Leverage resources such as the National Archives to categorize potential CUI received from key contractors. ✓ Develop a matrix to demonstrate the types of CUI related to each key contract. ✓ Discuss the CUI inventory with the program officers or contracting officer's technical representative (COTR) to confirm the existence and flow of CUI.
System consolidation: Identifying and taking an inventory of your covered contractual information systems (internal and external) and flow of information therein	▪ Business analyst ▪ IT project manager ▪ System architect	Annually	✓ Identify systems, applications and platforms that process, flow or transmit CUI both internally and externally. ✓ Develop a data flow diagram to illustrate the inflows and outflows of CUI in relation to key subcontractors and vendors. ✓ Consider reducing the scope and eliminating duplication of systems used to store, transmit and process CUI.
PHASE 2 — Assessment: Perform a readiness assessment to identify operational and technological improvement opportunities related to your organization's information security posture and your ability to align with CMMC security requirements.			
Gap assessment: Reviewing your systems, identifying gaps and validating your planned remediation strategy 	▪ Information security ▪ Internal audit ▪ Third-party assessor	Annually	✓ Perform an internal CMMC gap assessment of your organization's current-state information security program maturity. ✓ Leverage the identified gaps and recommendations to develop a remediation strategy.

PHASE 3 — Development: Develop a road map for closing identified gaps and establishing a sustainable security compliance program that supports continuous monitoring.			
Security program and design management: Building the policies, procedures, roles and responsibilities to protect CUI	▪ CISO ▪ Human resources ▪ Information security ▪ Legal	Quarterly	✓ Gain leadership commitment to allocate resources for CMMC compliance endeavors. ✓ Apply CMMC maturity recommendations to your program.
Employee awareness and training: Identifying employees who must access CUI, training them on the appropriate roles and responsibilities for handling and protecting data, and conducting background checks for employees and contractors	▪ CISO ▪ Human resources	Continuous	✓ Develop a mandatory training program for system users to understand their responsibility in CUI handling and marking. ✓ Require background checks for employees and contractors with access to systems containing CUI.
Configuration and hardening of systems: Defining security baselines, conducting vulnerability management and threat program exercises, and remediating deficiencies	▪ Information security ▪ Network administrators	Continuous	✓ Establish, maintain and review baseline configurations for covered contractor information systems. ✓ Establish, maintain and update system inventories to include detailed system metadata—hardware, software, firmware, and types of information stored therein.
Vendor management: Continuously monitoring your vendors, supply posture, and flow down of contractual requirements 	▪ Procurement ▪ Vendor management ▪ Vendors	Continuous	✓ Formalize the internal vendor risk management program to provide critical insight into the identification of third parties (e.g., subcontractors and vendors) and the effectiveness of third-party security risk management. ✓ Incorporate due diligence into the vendor selection process to include a CMMC-related security questionnaire. ✓ Identify vendor responsibilities and the flow down of cybersecurity requirements related to the CMMC
Continuous monitoring: Facilitating ongoing awareness of threats, vulnerabilities and information security to support organizational risk management decisions 	▪ CIO ▪ CISO ▪ Contracting officer ▪ Information security team	Continuous	✓ Perform internal audits and risk assessments to continuously evaluate the maturity of your cybersecurity program against the CMMC regulatory expectations. ✓ Develop, maintain and update a systems security plan (SSP) that reflects the current maturity of your organization's environment. ✓ Prepare to submit your self-assessed NIST SP 800-171 score to the supplier performance risk system (SPRS) database upon request. ✓ Update your self-assessment score every three years on the SPRS database.

Feeling overwhelmed? RSM's experienced advisors know what it takes to create and maintain a mature cybersecurity program and subsequently help you achieve CMMC certification. Contact us to discuss your organization's needs, and we'll help you chart, and execute, a path forward.

+1 800 274 3978
rsmus.com