RAPID7

BRIEF

Cybersecurity Maturity Model Certification (CMMC)

December 11, 2020

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a certification process, under development by the US Department of Defense (DoD), that requires certain cybersecurity practices for all contractors and subcontractors doing business with the DoD. Rapid7's solutions can help organizations prepare for and achieve CMMC compliance.

The certification requirement is expected to be phased into new DoD contracts over five years, starting in Q3 2020[1]. The contract will specify the level of CMMC certification required, and contractors must have the certification by time of contract award. Certified companies will need to recertify every three years, or potentially sooner if there are material changes to the organization's security posture. Note: The CMMC rules are continuing to evolve and may be updated in the future.

How to prepare for CMMC

While CMMC certification is not yet available, DoD encourages self-evaluations to help contractors be ready to successfully pass the independent assessment required for CMMC certification[2]. Assessing compliance with NIST SP 800-171 can also be a precusor to CMMC compliance, as the 800-171 security controls are incorporated in the CMMC[3].

Rapid7 can help organizations prepare for CMMC certification by evaluating their cybersecurity programs against the DoD's framework, identifying both gaps and areas of strength, using the same criteria that auditors will use. Rapid7's products and services can help organizations fulfill the practices and processes required under CMMC, including compliance with NIST SP 800-171, NIST SP 800-53, and other best practices that form the basis for the CMMC requirements[4].

[1] With the exception of contracts solely for commercial off-the-shelf items and contracts below the $10,000 micro-purchase threshold. See 85 Fed. Reg. 61507, 61520.
[2] There are presently no independent assessor organizations recognized by the CMMC Accreditation Body, and true CMMC certification is not yet available. However, DoD states that pre-assessment using the latest CMMC draft is "acceptable and encouraged." See https://www.cmmcab.org/faq.
[3] See CMMC v1.02, pgs. 10-11, https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf. In addition, DoD recently updated its acquisition rules to require, as part of new contracts and solicitations, contractors to assess their compliance with NIST SP 800-171. See 85 Fed. Reg. 61505-6. See also, pg. 9, https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf.
[4] See, for example, Rapid7's 800-171 compliance guide: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-nist-800-171-compliance-guide.pdf.

What CMMC requires

CMMC establishes five levels of cybersecurity maturity, with each level requiring compliance to both *practices* and *processes*. DoD contract RFIs will specify the precise certification level needed for a contract award.

Across the five levels, there are a total of 171 cybersecurity *practices* to be implemented as cybersecurity controls. The *processes* required at each level will be evaluated by how well the controls are institutionalized in the organization and embedded in its operations[5]. The practices and processes are cumulative - lower level requirements are also required in upper levels.

- **Level 1:** *Basic Cyber Hygiene.* Nearly all DoD contractors must certify at Level 1 or above. This level requires contractors to apply 17 cybersecurity practices.[6] These basic practices include, for example, identifying and reporting information system flaws in a timely manner (see CMMC control SI.1.210).[7] Process maturity is not assessed at this level.

- **Level 2:** *Intermediate Cyber Hygiene.* This level is a transition stage between Levels 1 and 3. This level requires 72 total practices, such as detecting and reporting cybersecurity events (IR.2.093). To meet level 2 process requirements, contractors must document their practices.

- **Level 3:** *Good Cyber Hygiene.* All contractors that handle any Controlled Unclassified Information (CUI) must certify at Level 3 or above.[8] This level requires 130 practices, such as periodically performing risk assessments to identify and prioritize cybersecurity risks (RM.3.144). To meet process requirements, contractors must demonstrate a management plan for implementing the practices.

- **Level 4:** *Proactive.* This level requires 156 practices, such as conducting periodic penetration tests leveraging automated scanning tools (CA.4.164). To meet process requirements, contractors must review and measure their practices for effectiveness.

- **Level 5:** *Advanced/Progressive.* This level requires 171 practices, such as ongoing monitoring of system components for anomalous or suspicious behavior (SI.5.223). To meet process requirements, contractors must standardize and optimize practice implementation across the organization.

[5] See pgs. 6-7: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf.
[6] See CMMC Model v1.02, pg. 10. See also 48 CFR 52.204-21.
[7] See CMMC Model Matrix v1.02, https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf.
[8] See CMMC Model v1.02, pg. 4.

Our solutions

CMMC's 171 security practices are organized into 17 domains, with each domain representing a general category of cybersecurity control. Rapid7's solutions can help you meet the practices in each of the CMMC domains, as well as other cybersecurity standards and regulatory requirements. Below is a brief overview of key Rapid7's products and services, as well as a chart showing which solutions can help fulfill each CMMC domain.

InsightVM

Rapid7 InsightVM[10] or our managed version, MVM[11], allow you to conduct frequent vulnerability assessments and identify the assets that pose the most risk by using exploitability, malware exposure, and vulnerability age to show you which assets would be easiest to breach in an attack (and how to fix them).

InsightIDR

Using InsightIDR[12] or our managed version, MDR[13], and our ability to correlate LDAP, Active Directory, and DHCP not only helps identify and keep track of all assets in your environment, but can also identify unauthorized access and other malicious behavior through our user behavior analytics, deception technology, and agents.

InsightAppSec

With InsightAppSec[14], or Managed Insight AppSec (MAS) Rapid7 brings proven Dynamic Application Security Testing (DAST) technology to the Insight platform. InsightAppSec combines powerful application crawling and attack capabilities, flexibility in scan scope and scheduling, and accuracy in results with a modern UI, intuitive workflows, and sensible data organization.

Web applications are not monolithic. They have decoupled front ends that interface with micro-services that transact with the backend, as well as multiple development, pre-production, and production environments. InsightAppSec provides the flexibility to configure scans to optimize coverage and testing for each individual aspect of an application, whether it's an API or a Single Page Application (SPA) front end.

Managed Services

Our portfolio of Managed Services[15] is designed to support organizations identifying and remediating risks and ensures a layered approach to defend against advanced threats. We have over 20 years of experience helping organizations advance securely by reducing the complexities of building a holistic security program. Our team of expert researchers, analysts, and advisors extend your team by providing the resources needed to advance your program, improve your security posture, and confidently respond to threats.

[9]The 17 CMMC domains are 1) Access Control, 2) Asset Management, 3) Audit and Accountability, 4) Awareness and Training, 5) Configuration Management, 6) Identification and Authentication, 7) Incident Response, 8) Maintenance, 9) Media Protection, 10) Personnel Security, 11) Physical Protection, 12) Recovery, 13) Risk Management, 14) Security Assessment, 15) Situational Awareness, 16) Systems and Communications Protection, and 17) Systems and Information Integrity. See CMMC Model v1.02, pg. 7.
[10]https://www.rapid7.com/products/insightvm/
[11]https://www.rapid7.com/services/managed-services/vulnerability-management/
[12]https://www.rapid7.com/products/insightidr/
[13]https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/
[14]https://www.rapid7.com/products/insightappsec/ Further Reading

DivvyCloud by Rapid7

DivvyCloud[16] provides an automated platform to analyze, identify, and remediate cloud infrastructure using customer-definable rules and actions. Once installed, configured, and connected to an organization's clouds, DivvyCloud discovers infrastructure resources across all clouds and distills this information into a normalized database. This database is used to analyze cloud operations, identify risks, and take actions.

DivvyCloud's extensible platform is designed to enable organizations to securely embrace public cloud and containers, giving developers the freedom to innovate without exposing the business to risk. Customers use DivvyCloud's real-time remediation to achieve continuous security and compliance in Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, Kubernetes, and other environments.

Penetration Testing Services

Rapid7's Penetration Testing Services[17] give you a real-world look at how attackers could exploit your vulnerabilities – and guidance on how to stop them. Our team not only performs more than 1,000 penetration tests every year, but is also dedicated to ongoing security research, making them as close to real-world hackers as you can get. Rapid7 PenTesting is a critical resource to inform your overall security posture, but also to help meet the Identification and Authentication as well as the Risk Management controls CMMC requires.

Advisory Consulting Services

Rapid7's Advisory Consulting Services [18]provide assessment and development services that give you the steps—and confidence—you need to take your security program to the next level. Our team of experts have decades of security, risk, and IT experience across different industries and company sizes. They have an innate drive to make your security programs relevant, actionable, and sustainable. Powered by our people and our leading technology, Rapid7's Advisory Consulting Services can help organizations meet every CMMC domain with our Readiness Assessment that can provide a clear pathway to resolve POAM findings before an organization undergoes the required certification process[19].

Incident Response Services

With our Incident Response Services[20], Rapid7 is ready to collaborate closely with your in-house team to detect threats, document findings, and recommend the right remediation activities to help ensure attackers are out and can't find their way back in. Rapid7 IR Services can conduct table-top exercises, breach readiness assessments, and implement an IR program suited for your company. These services prepare you to demonstrate diligence with the Incident Response and Risk management requirements of CMMC.

[16]https://www.rapid7.com/products/divvycloud/

[17]https://www.rapid7.com/services/security-consulting/penetration-testing-services/

[18]https://www.rapid7.com/services/security-consulting/security-advisory-services/

[19]In areas where Rapid7 does not offer a solution directly, such as Personnel Security, our Advisory Services can help guide organizations to trusted service providers.

[20]https://www.rapid7.com/services/security-consulting/incident-response-services/

Mapping Rapid7's solutions to CMMC domains

Below is an overview of how Rapid7's solutions can help organizations meet the 17 CMMC domains. Each of the products and services help organizations address their compliance needs in specific ways. Give us a call to learn more!

CMMC domain	InsightVM	InsightIDR	InsightAppSec	DivvyCloud	Penetration Testing Services	Advisory Services	Incident Response Services
Access Control	X	X		X		X	
Asset Management	X			X		X	
Audit and Accountability		X		X		X	
Awareness and Training						X	X
Configuration Management	X	X		X		X	
Identification and Authentication		X		X	X	X	
Incident Response		X				X	X
Maintenance				X		X	
Media Protection				X		X	
Personnel Security						X	
Physical Protection						X	
Recovery						X	
Risk Management	X		X	X		X	
Security Assessment	X	X	X	X	X	X	
Situational Awareness				X		X	
Systems and Communications Protection	X	X	X	X		X	
System and Information Integrity	X	X	X	X		X	

Further reading

- Dept. of Defense, CMMC Model v1.02 and overview briefing[21]
- Dept. of Defense, Levels 1 and 3 Assessment Guides[22]
- Rapid7, Preparing for the Cybersecurity Maturity Model Certification, Part 1[23]
- Rapid7, Preparing for the Cybersecurity Maturity Model Certification, Part 2[24]
- Rapid7, NIST SP 800-171 Compliance Guide[25]
- Dept. of Defense, NIST SP 800-171 Assessment Methodology[26]
- Dept. of Defense, Interim Rule, DFARS Assessing Contractor Implementation of Cybersecurity Requirements[27]

[21] https://www.acq.osd.mil/cmmc/draft.html

[22] https://www.acq.osd.mil/cmmc/docs/CMMC_AG_L1_20201125.pdf and https://www.acq.osd.mil/cmmc/docs/CMMC_AG_L3_20201130.pdf

[23] https://blog.rapid7.com/2020/04/15/preparing-for-the-cybersecurity-maturity-model-certification-cmmc-part-1-practice-and-process/

[24] https://blog.rapid7.com/2020/05/11/preparing-for-the-cybersecurity-maturity-model-certification-cmmc-part-2-the-larger-picture/

[25] https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-nist-800-171-compliance-guide.pdf

[26] https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementa-

About Rapid7

Organizations around the globe rely on Rapid7 technology, services, and research to securely advance. The visibility, analytics, and automation delivered through our Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Support

call +1.866.380.8113

Customer Portal