CMMC Compliance: The Essential Guide

Navigating cybersecurity compliance in the defense sector

eBook

KEYSIGHT

Contents

CHAPTER 1

What Is Cybersecurity Maturity Model Certification (CMMC)?

CHAPTER 1

What Is Cybersecurity Maturity Model Certification (CMMC)?

The defense industrial base (DIB) is the industrial network that provides research and development for weapons systems, subsystems, and components. Because of its close connections to the military and national security, it faces increasingly frequent and sophisticated cyberattacks. To safeguard American innovation and national security information residing on DIB systems and networks, the Department of Defense (DOD) established the Cybersecurity Maturity Model Certification (CMMC) program.

The DOD aligns CMMC with its information security requirements for DIB partners. CMMC serves as a verification tool, ensuring that contractors, subcontractors, and university researchers meet the cybersecurity requirements for protecting controlled unclassified information (CUI) and federal contract information (FCI). Under the DFARS Cybersecurity Proposed Rule, contractors must achieve CMMC certification at the time of contract award and maintain it for the contract's duration after a phase-in period. Additionally, senior company officials must provide a new security affirmation for any security change.

Navigating federal protocols or processes

The US government creates or provides Federal Contract Information (FCI) for developing or delivering a product or service, but the information is not for public release.

FCI includes information such as the following:

- contract performance reports
- emails
- invoices and payment information
- past performance details
- process documentation

CUI encompasses information that needs protection or controlled dissemination according to federal laws, regulations, and government-wide policies. In short, all CUI held by a government contractor or researcher is FCI, but not all FCI is CUI. Identifying CUI will initially present a significant challenge for contractors when implementing the necessary cybersecurity controls.

Who needs certification?

The DOD requires contractors, subcontractors, and university researchers who process, store, or transmit FCI or CUI to obtain CMMC certification. Contractors must ensure that CMMC certification requirements flow down to subcontractors at all tiers when they handle the same information. While we anticipate the establishment of rules for verifying subcontractors' compliance, contractors lack access to their subcontractors' Supplier Performance Risk System scores. For now, contractors must rely on other methods to confirm compliance, such as obtaining a screenshot of the scores or an attestation from the subcontractor.

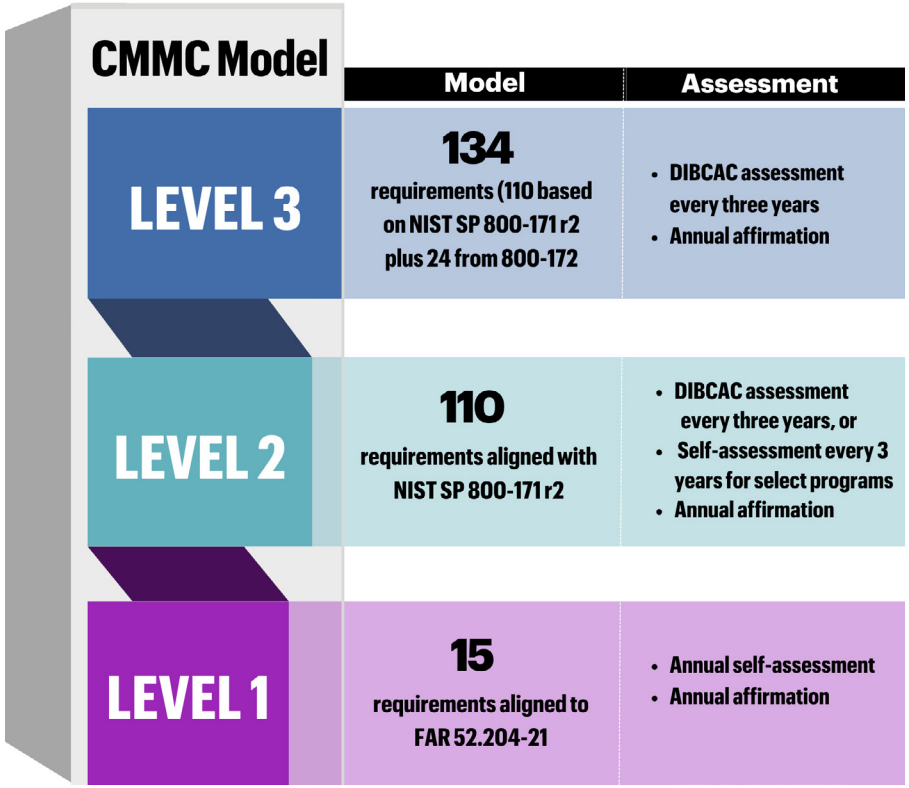
The evolution to CMMC 2.0

CMMC 1.0, released in 2020, included five maturity levels and lacked self-certification. After an internal review and public comments on CMMC 1.0, the DOD launched CMMC 2.0 in November 2021. The goals of the program include the following:

- Safeguarding sensitive information to enable and protect warfighters.
- Enforcing DIB cybersecurity standards to meet evolving threats.
- Ensuring accountability while minimizing barriers to compliance with DOD requirements.
- Perpetuating a collaborative culture of cybersecurity and cyber resilience.
- Maintaining public trust through high professional and ethical standards.

This initiative underscores the critical role of DIB cybersecurity in protecting the information that supports and empowers our warfighters.

CMMC model



Key features of CMMC

- **Tiered, progressive model:** Depending on the type and sensitivity of the information, the CMMC requires that companies implement standards at progressively advanced levels.
- **Assessment requirement:** The DOD will verify the cybersecurity standards via third-party assessments or self-assessments.
- **Contract implementation:** The DOD requires contractors dealing with CUI to achieve a particular CMMC level as a prerequisite for contract allocation.
- **Assessment requirement:** CMMC assessments enable the DOD to verify the implementation of clear cybersecurity standards.
- **Implementation through contracts:** Once CMMC reaches full implementation, the DOD will require certain contractors handling sensitive CUI to achieve a particular level as a condition of contract award.

CMMC acronyms

	Description
FCI	Federal contract information
CUI	Controlled unclassified information
CMMC	Cybersecurity maturity model certification
DIB	Defense industrial base
DOD	Department of defense
SPRS	Supplier performance risk systems
CFR	Code of federal regulation
C3PAO	CMMC third party assessment organization
APT	Advanced persistent threat
NIST	National institute of standard and technology
DIBCAC	Defense industrial base cybersecurity assessment center
LTP	Licensed training providers
TTP	Tactics, techniques and procedures
ATI	Application and threat intelligence
BAS	Breach and attack simulation
SOC	Security operations center
IoT	Internet of Things
FIPS	Federal information processing standard
DoDIN APL	DOD information approved products list

Certification timeline

The DOD completed rulemaking rulemaking in November 2024, including a comprehensive cost analysis for each level of CMMC. The costs should be lower than CMMC 1.0 because the DOD streamlined requirements, eliminating unique practices and maturity processes. It also allowed companies at Level 1 and some at Level 2 to perform self-assessments instead of third-party assessments.

CMMC assessments start in Q125. Since the DOD has finalized the CMMC proposed rule, defense contractors could see CMMC requirements phased into their contracts by spring 2025. The time between solicitation and contract award is usually one month, so there will not be time for contractors and subcontractors to get certified once they bid. They must achieve certification before they bid on a contract.

- Contractors can expect the certification process to take an average of two and a half years — 12-18 months for preparation and 9-15 months for assessment. Companies that haven't yet started the process now are risking their defense contracts, business reputation, steep fines, and regulatory compliance. Compliance and certification will not be a one-time event but an ongoing process with regular recertification, notification of changes and breaches, and addressing any enhanced notification requirements. As a result, DD contractors and subcontractors must prioritize cybersecurity every day.

Companies that haven't yet started the process are risking their defense contracts, business reputation, steep fines, and regulatory compliance.

The benefits of certification

Organizations aiming to enhance their cybersecurity posture and gain a competitive edge in government contract bidding receive numerous advantages from CMMC certification.

Increased competitiveness

With CMMC certification, your organization retains its ability to bid on DOD contracts and becomes even more competitive. Certified contractors receive prioritization from many government agencies, including the DOD. Obtaining CMMC certification gives you a distinct advantage over uncertified competitors, increasing your chances of securing lucrative government contracts.

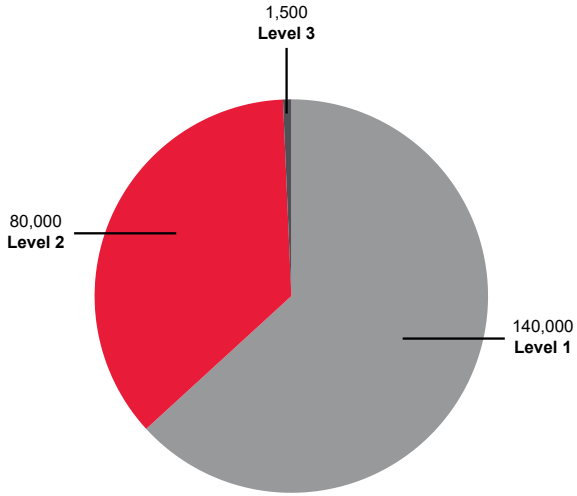
Absolute trust and credibility

Your organization builds trust and credibility with the DOD and other stakeholders through CMMC certification. The certification proves your organization's commitment to maintaining a high level of cybersecurity. You establish a reputation as a trusted partner by demonstrating your dedication to protecting sensitive data, opening doors to new opportunities and collaborations.

Enhanced cybersecurity posture

Your organization demonstrates its commitment to implementing robust cybersecurity controls by achieving CMMC certification. By adhering to the stringent requirements of CMMC, you can fortify your defenses against cyberthreats and protect sensitive information.

Number of companies at each CMMC level



DoD estimate of more than 220,000 defense industrial base companies

CHAPTER 2

Certification Levels Explained

CHAPTER 2

Certification Levels Explained

CMMC comprises three levels based on the type of information an organization handles. Contractors, subcontractors, and university researchers handling FCI should aim for Level 1. Those managing CUI should pursue Level 2 certification. The DOD requires organizations involved in its most sensitive projects to attain Level 3 certification.

Level 1

This Foundational level applies to contractors or subcontractors who process, store, or transmit FCI on unclassified contractor information systems. While FCI is not as sensitive as CUI, it still requires protection. CMMC Level 1 is also known as basic cyber hygiene. It requires 15 basic safeguarding practices based on the 48 Code of Federal Regulation (CFR) 52.204-21. One example includes limiting information system access to authorized users, processes acting on behalf of authorized users, or devices.

Level 1 organizations may conduct an annual self-assessment and attestation instead of hiring a third party. The DOD estimates that the majority of the DIB will fall under this level.

Level 2

CMMC Level 2 applies to organizations processing, storing, or transferring CUI on unclassified contractor information systems. This information requires safeguarding and may also be subject to dissemination controls. The DOD estimates that 36% of the DIB will fall into Level 2.

CMMC Level 2 is considered the Advanced level and encompasses 110 requirements based on NIST SP 800-171r2. Each level is progressive, so Level 2 requires all of Level 1 plus the new practices.

A company at this level must receive an assessment every three years conducted by an accredited CMMC third-party assessment organization (C3PAO). After completing the CMMC assessment, the C3PAO will provide a report to Cyber AB, CMMC's official accreditation body. An annual self-attestation will also be necessary to confirm that the company still meets CMMC requirements.

The DOD allows an estimated 5% of Level 2 organizations to perform annual self-assessments instead of using a third party. This subset includes contractors handling CUI but working on projects that do not involve sensitive national security information, also known as nonprioritized acquisitions.

Level 3

The DOD continues to develop this level, which will be determined on a contract-by-contract basis, depending on the sensitivity of the CUI involved. This level, reserved for the highest-priority programs, focuses on decreasing the risk from advanced persistent threats (APTs). The DOD estimates that only 1% of the DIB will be Level 3.

Known as the Expert level, Level 3 will include the more than 110 requirements from NIST SP 800-171r2 plus the enhanced security requirements in NIST SP 800-172.

The Defense Industrial Base Cybersecurity Assessment Center must assess companies at this level every three years. Another requirement will be an annual self-attestation to confirm they still meet CMMC requirements.

CHAPTER 3

Core Security Domains of CMMC

Core Security Domains of CMMC

The CMMC framework groups security practices into distinct domains with similar attributes, which is key to protecting FCI and CUI. The CMMC framework includes 14 core domains that align with the families of security requirements specified in NIST SP 800-171r2:

CMMC security requirement families

Accessc control	Media protection
Awareness and training	Personal security
Audit and accountability	Physical protection
Configuration management	Risk assessment
Identification and authentification	Security assessment
Incident response	System and communication protection
Maintenance	System and information integrity

Access control

The access control domain outlines requirements for managing accounts in CUI systems. It covers topics such as the following:

- Defining account types.
- Creating and managing accounts.
- Authorizing access.
- Monitoring account usage.
- Deactivating accounts when necessary.

Awareness and training

The awareness and training domain summarizes the requirements for security literacy and role-based training. It covers topics such as the following:

- Providing initial and ongoing training to system users.
- Updating training content and conducting awareness training to address insider threats.
- Addressing social engineering.
- Safeguarding against social mining.

Audit and accountability

The audit and accountability domain encompasses the selection of event types for logging, generation of audit records, and retention of audit records. It covers topics such as the following:

- Selecting appropriate event types.
- Generating audit records at the appropriate level of abstraction.
- Retaining audit records for a specified time.

Configuration management

The configuration management domain specifies requirements for developing, maintaining, reviewing, and updating the baseline. It covers topics such as the following:

- Establishing configuration settings.
- Controlling configuration changes.
- Analyzing security impacts.
- Defining access restrictions.
- Configuring systems for high-risk areas.

Identification and authentication

The identification and authentication domain details the use of strong authentication methods, reauthenticating users when necessary, and protecting against replay attacks. It covers topics such as the following:

- Identifying and authenticating users and devices.
- Using multifactor authentication.
- Implementing replay-resistant authentication mechanisms.

Incident response

The incident response domain breaks down incident response in CUI systems. It covers topics such as the following:

- Implementing an incident-handling capability.
- Monitoring and reporting incidents.
- Testing the effectiveness of incident response.
- Developing an incident response plan.

Maintenance

The maintenance domain outlines maintenance tools in CUI systems. It covers topics such as the following:

- Approving and monitoring the use of maintenance tools.
- Checking media for malicious code.
- Preventing the removal of maintenance equipment.

Media protection

The media protection domain identifies how to secure media. It covers topics such as the following:

Physically controlling and securing media.

- Restricting access to media.
- Sanitizing media before disposal or reuse.

Personnel security

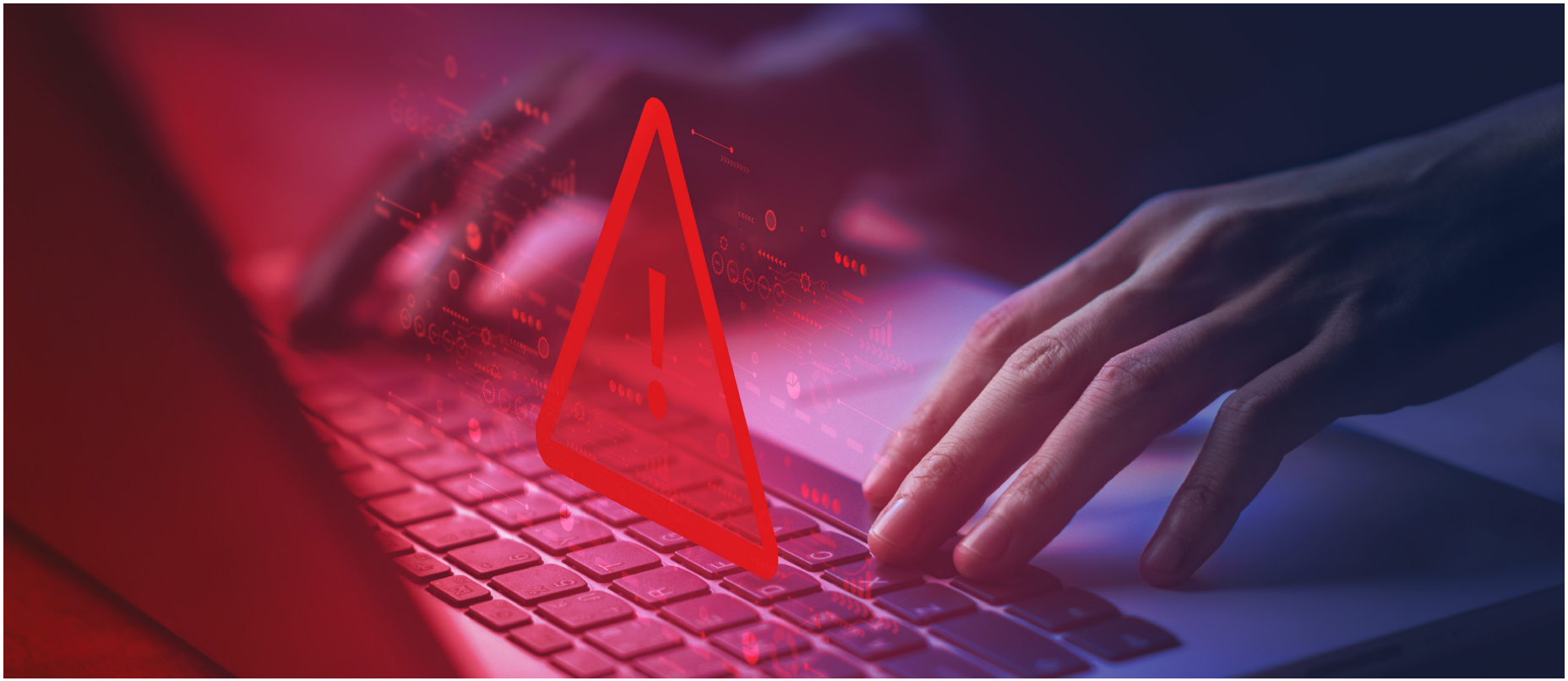
The personnel domain establishes the benchmarks for personnel. It covers topics such as the following:

- Screening individuals prior to authorizing access.
- Terminating and transferring individuals.
- Ensuring the security of personnel-related system property.

Physical protection

The physical protection domain provides details on physical access to buildings and equipment. It covers topics such as the following:

- Developing and maintaining a list for authorized access.
- Issuing authorization credentials.
- Monitoring physical access.
- Controlling physical access to output devices.



Risk assessment

The risk assessment domain delineates the process of conducting risk assessments at different levels. It covers topics such as the following:

- Assessing the risk of unauthorized disclosure.
- Updating risk assessments.
- Responding to findings from security assessments.

Security assessment and monitoring

The security assessment and monitoring domain highlights key security components. It covers topics such as the following:

- Assessing security requirements.
- Developing a plan of action and milestones.
- Implementing a continuous monitoring strategy.
- Conducting security assessments.
- Documenting results.

System and communications protection

The systems and communications protection domain enumerates boundary protection measures. It covers topics such as the following:

- Monitoring managed interfaces.
- Using demilitarized zones for publicly accessible systems.
- Preventing unauthorized information transfer in shared resources.
- Denying network communication by default.
- Enforcing confidentiality through encryption.

System and information integrity

The system and information integrity domain details ongoing system integrity and security. It covers topics such as the following:

- Installing security updates within a defined time frame.
- Implementing mechanisms to detect and eradicate malicious code at system entry and exit points.
- Configuring mechanisms to block or quarantine threats.
- Disseminating security alerts and directives.

CHAPTER 4

Tools and Solutions to Help

CHAPTER 4

Tools and Solutions to Help

At Keysight, we understand the significance of CMMC certification and its impact on your organization's success. Our range of cutting-edge cybersecurity solutions can assist you in meeting CMMC requirements and streamlining the certification process. With our expertise and advanced technology, you can confidently achieve CMMC certification and leverage its benefits to drive growth and secure valuable government contracts.

Here is a closer look at the Keysight cybersecurity solutions designed to help organizations achieve CMMC certification and streamline the certification process.

Breach and attack simulation tools

A state-of-the-art breach and attack simulation (BAS) platform, like Keysight Threat Simulator (Figure 2), can mimic cyberattacks on your network, revealing potential vulnerabilities and assessing the impact of different security breaches. Your team can prioritize its efforts and bolster system defenses using comprehensive reports that highlight critical areas needing immediate attention. Additionally, BAS platforms let you conduct regular assessments, making it easy to proactively monitor your security posture.

For CMMC Level 2, which requires configuration management, incident response, and security assessment (CMMC security requirements 3.4, 3.6, and 3.12), a BAS platform covers these effectively. Level 3 certification demands additional security practices like risk assessment and system and communications protection practices (CMMC security requirements 3.11 and 3.13). The platform facilitates these advanced requirements by continuously testing and improving your security posture, ensuring compliance and robust protection against cyberthreats.

Keysight Threat Simulator

Figure 2. Keysight Threat Simulator

Configuration management	Incident response	Risk assessment	Security assessment	System and information integrity

Cybersecurity training platform

A comprehensive cybersecurity training platform can significantly aid certification, particularly at Levels 2 and 3. Having a platform like Keysight Cyber Range (Figure 3) to practice responses to realistic, simulated scenarios of cyberthreats helps meet the incident response domain (CMMC security requirement 3.6) of CMMC. Additionally, specialized training on security operations center (SOC) procedures — including threat detection, incident analysis, and response coordination — ensures compliance with the SOC training domain for CMMC. This holistic approach to training simplifies and speeds certification while significantly strengthening your organization's cybersecurity posture.

Keysight Cyber Range

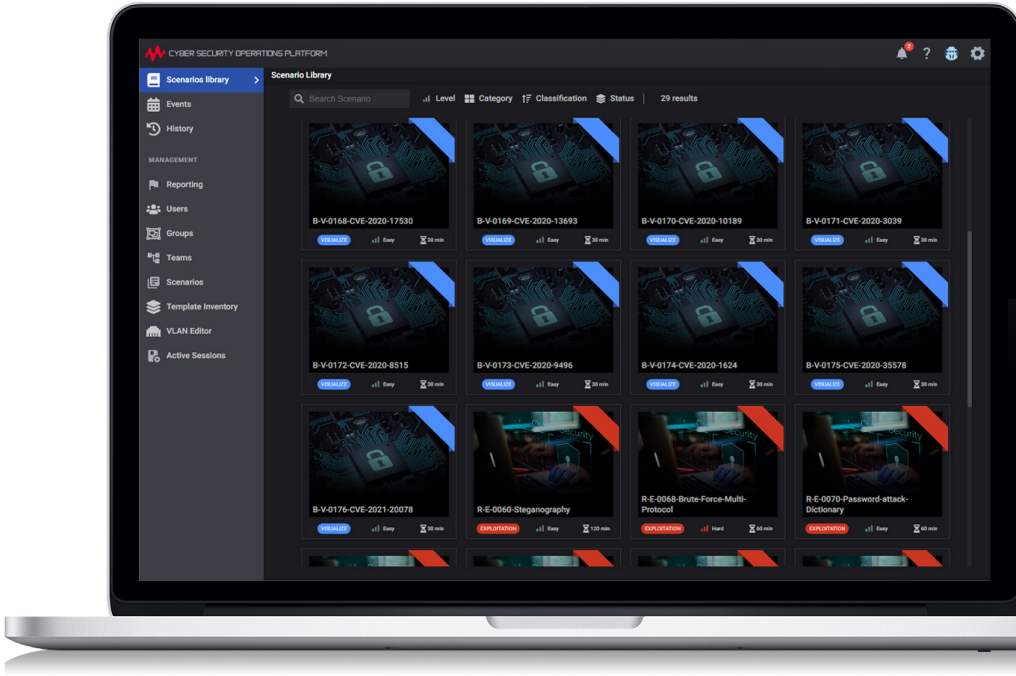


Figure 3. Keysight Cyber Range

Network performance and security testing solutions

Network performance and security testing solutions, such as Keysight CyPerf and Keysight BreakingPoint, are crucial in meeting CMMC domains for all levels. This process requires analyzing the security impact of changes before implementing them in the configuration management domain (CMMC security requirement 3.4).

Along with testing the robustness of authentication mechanisms and reviewing access control processes, this requirement is essential for ensuring that only authorized individuals have access to CUI.

It ensures that they can perform their assigned tasks while preventing unauthorized access. You must validate the effectiveness of your security controls by simulating attacks and monitoring the response, be aware of threats, and protect your system and communications (CMMC security requirement 3.12) from techniques of misdirection and deception.

Access control	Configuration management	Identification and authentication	Risk assessment	Security assessment

Keysight CyPerf and Keysight Breaking Point

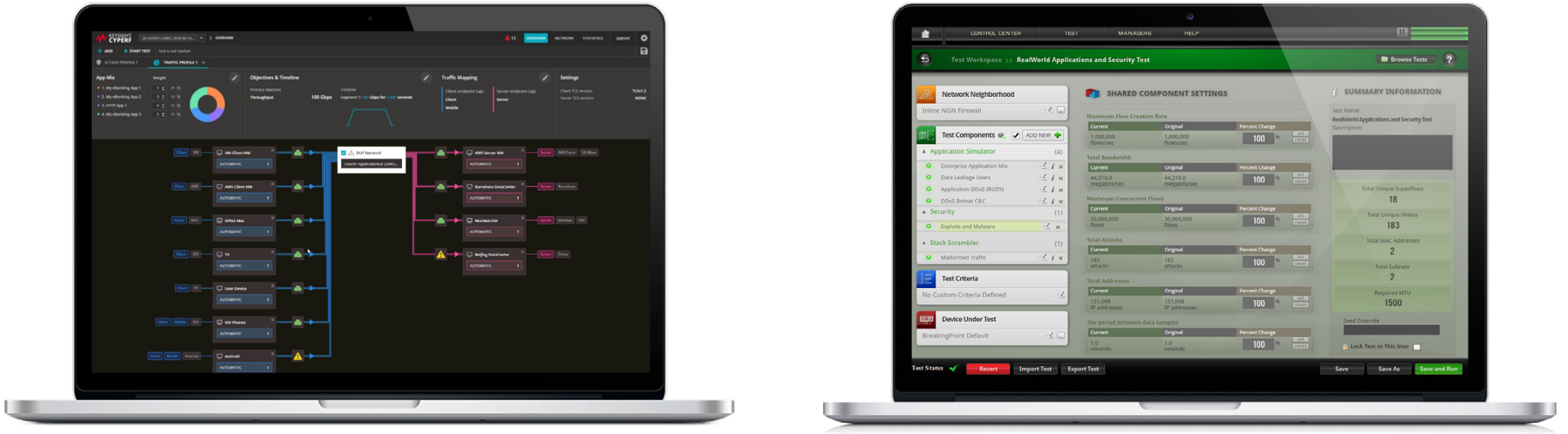


Figure 4. Keysight CyPerf and Keysight Breaking Point

IoT security testing platform

An Internet of Things (IoT) security testing platform is instrumental in achieving all three levels of certification across the four key domains. CMMC mandates robust practices in vulnerability management, incident response, and network segmentation (CMMC security requirement 3.6), and a powerful tool like Keysight IoT Security Assessment (Figure 5) fits the bill. IoT security testing platforms for connected devices on the network secure consumer and industrial devices, including operational technology and Industrial IoT systems like thermostats, industrial controllers, robot factory arms, security cameras, and badge scanners. These platforms ensure that such devices comply with the standards.

The platform generates detailed reports and logs that serve as evidence of compliance. This documentation is crucial during the certification audit process. Additionally, it enhances vulnerability management, designs for resiliency, detects misconfigurations, and ensures proper network segmentation. These capabilities are critical for achieving and maintaining certification.

Keysight IoT Security Assessment

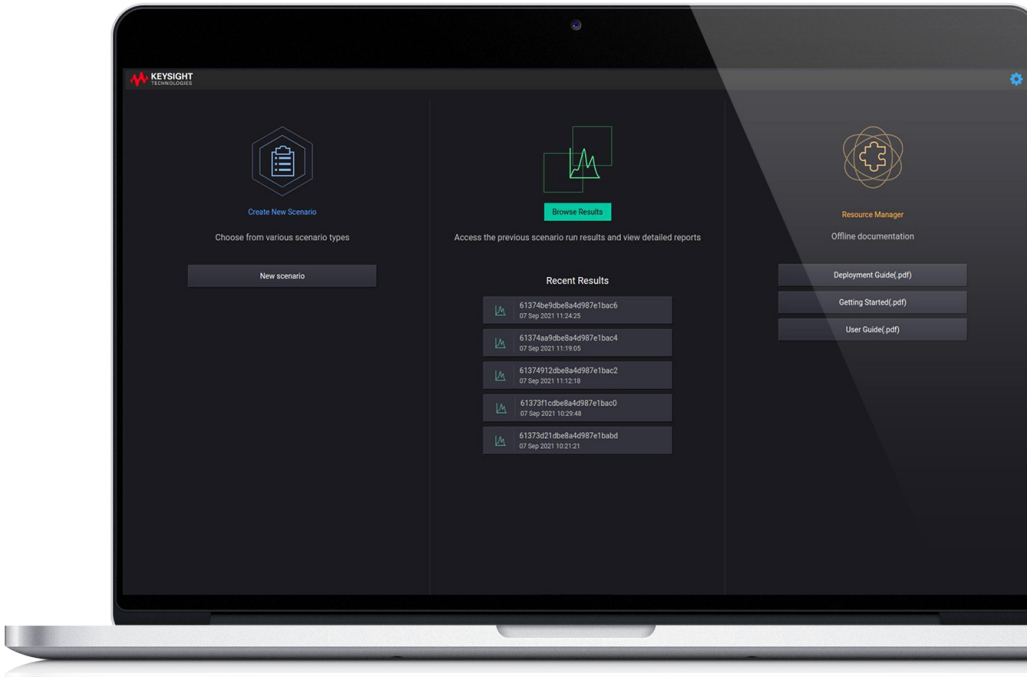


Figure 5. Keysight IoT Security Assessment

Risk assessment

Software test platform

Advanced testing and automation capabilities can streamline the process of achieving CMMC certification. Automated testing tools help validate security controls, ensuring that they meet stringent requirements, including testing for vulnerabilities and ensuring compliance with necessary security standards. This process meets the security assessment domain of CMMC (CMMC security requirement 3.12)

Continuous monitoring capabilities are essential for maintaining compliance over time, enabling organizations to quickly identify and address any security issues that may arise. Comprehensive reporting features document compliance efforts and results, which are crucial for the CMMC assessment process, providing clear evidence of compliance and areas needing improvement. An automated testing tool, like Keysight Eggplant (Figure 6), exemplifies these capabilities, offering a robust solution for organizations aiming to achieve and maintain CMMC compliance.

Keysight Eggplant Test

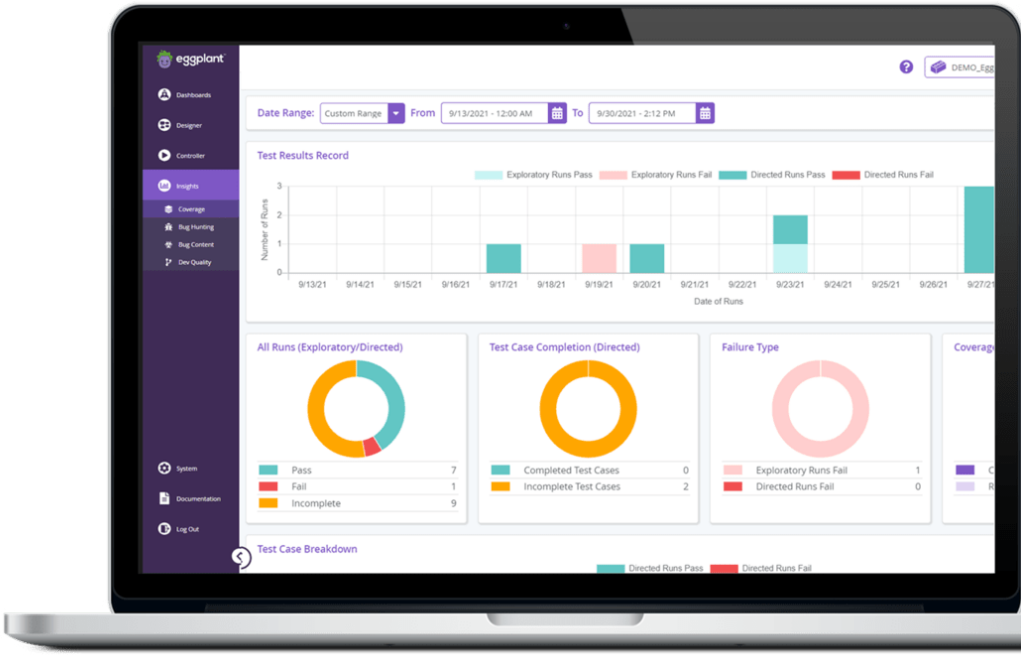


Figure 6. Keysight Eggplant Test

Identification and authentication

Network visibility solutions

Defense contractors rely on network traffic management devices like Keysight network packet brokers (NBPs) (Figure 7) with physical and virtual taps to secure their networks. These devices address nine required practices across all certification levels, providing robust boundary protection to control the flow of CUI and managing and monitoring sensitive data.

With system auditing capabilities that leverage data from physical taps, as well as insights from virtualized environments, these devices ensure thorough communications tracking and accountability. In terms of incident response (CMMC security requirement 3.6), these devices enable the ability to quickly identify and handle incidents by monitoring traffic in real time for signs of compromise or attack. Security control monitoring (CMMC Security Requirement 3.12) becomes more efficient as these devices continuously assess the security posture of the network through traffic filtering and forwarding. The insights provided enable incident response teams to promptly identify threats. From audit and accountability to system and information integrity, Keysight NPBs with taps are key tools to aid your CMMC certification.

Incorporating these solutions into your security arsenal will help you achieve certification before the 2026 deadline. These essential tools will streamline your path to CMMC certification, enhance your cybersecurity posture, protect sensitive defense information, and give you a competitive advantage.

Keysight Network Packet Brokers and Taps

Figure 7. Keysight Network Visibility Solutions

The Benefits of Using Technology for CMMC Certification

By leveraging these seven essential tools, organizations needing to meet CMMC can achieve significant benefits, including these:

- **Enhanced security posture:** Better protect sensitive information with specialized cybersecurity tools, aligning with CMMC requirements.
- **Faster certification process:** Streamline compliance efforts and reduce the time needed to prepare for and achieve certification.
- **Easier compliance management:** Simplify the management of compliance requirements with features like automated tracking, reporting, and documentation.
- **Improved accuracy and consistency:** Perform all compliance activities consistently and accurately to minimize the risk of human error.
- **Efficient resource use:** Use automation and streamlined processes to reduce the need for extensive personnel and enable more effective resource allocation.
- **Better preparedness for audits:** Maintain thorough records and documentation, making it easier to demonstrate compliance during audits.

CHAPTER 5

Steps to Prepare for CMMC Certification

CHAPTER 5

Steps to Prepare for CMMC Certification

Navigating the complexities of CMMC certification can be challenging, especially with evolving requirements and new regulations. This chapter outlines the essential steps to prepare for certification, ensuring your organization will be well-equipped to meet the standards.

Establish a strong cybersecurity culture

Foster a culture of awareness and accountability throughout your organization with regular training and communication on cybersecurity best practices. Many licensed training providers offer programs for CMMC certification.

Update and patch systems regularly

Keep your systems and software up to date with the latest security patches to mitigate potential vulnerabilities. Additionally, establish a schedule for these updates to ensure that you don't miss any critical patches and that you document everything.

Identify the appropriate CMMC level for your organization

Level 1 is for contractors, subcontractors, and university researchers handling FCI. Level 2 is for those managing CUI. Only organizations involved in the DOD's most sensitive projects must attain Level 3 certification.

Understand the requirements for your CMMC level

Study the CMMC framework to understand the specific controls and practices necessary for compliance. Regularly visit the DOD's CMMC website and Cyber AB's website to stay informed about the latest developments.

Assess your current cybersecurity posture

Evaluate your existing security practices and identify any gaps or vulnerabilities. Identify who within your organization has access to CUI, which devices are used for processing CUI, and which organizational procedures pertain to safeguarding CUI.

Select a C3PAO and complete a readiness assessment

Early adopters will have their choice of C3PAO. Late movers might not be as fortunate. With only 57 C3PAOs available and thousands of companies needing assessment, those who do not plan will face substantial wait times.

Onboard tools and solutions to secure your data

Cybersecurity solutions like the Keysight portfolio of network and data center security and network visibility products can help you secure your FCI and CUI to meet the majority of CMMC domain requirements.

Develop a compliance plan

Create a roadmap outlining the steps to meet CMMC requirements, including assigning responsibilities and setting deadlines. A useful step is to diligently record your reasoning and interpretations of the as-yet-undefined aspects of CMMC.

Implement necessary controls

Implement the controls specified in the CMMC framework, such as access control, incident response, and system and communications protection. Onboard new tools and solutions to help, like network monitoring and threat intelligence platforms.

Conduct regular audits and assessments

Continuously monitor and evaluate your compliance efforts to ensure ongoing adherence to CMMC requirements. Regularly review and update the controls to ensure they remain effective against evolving threats.

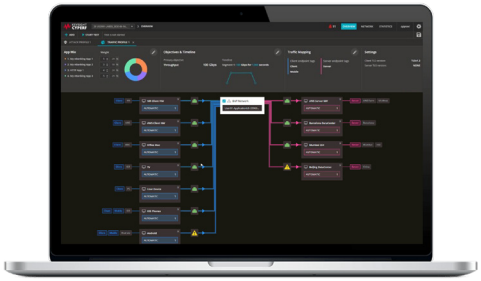
Partner with your C3PAO on the official CMMC assessment

The process could take up to 18 months. During this period, it is crucial to maintain open communication with your C3PAO to ensure that you are meeting all requirements and properly preparing documentation.

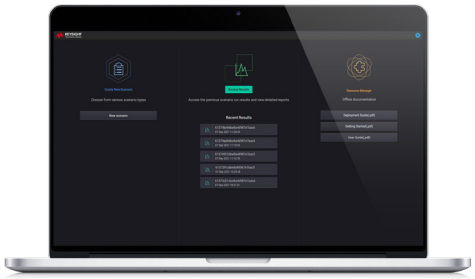
Learn more

Keysight solutions meet a comprehensive range of CMMC standards and guidelines, streamlining your certification process without the hassle of managing multiple vendors. Empowering companies to meet CMMC requirements more efficiently and cost-effectively, Keysight helps strengthen security posture, simplifies compliance management, improves resource utilization, and enhances audit preparation. As a trusted partner of US defense contractors, Keysight has extensive experience obtaining and maintaining federal risk mitigation certifications, such as Common Criteria, FIPS 140-2, and DoDIN APL.

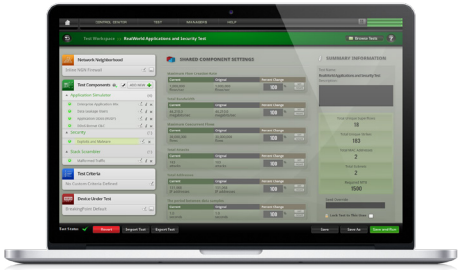
Keysight Treat Simulator



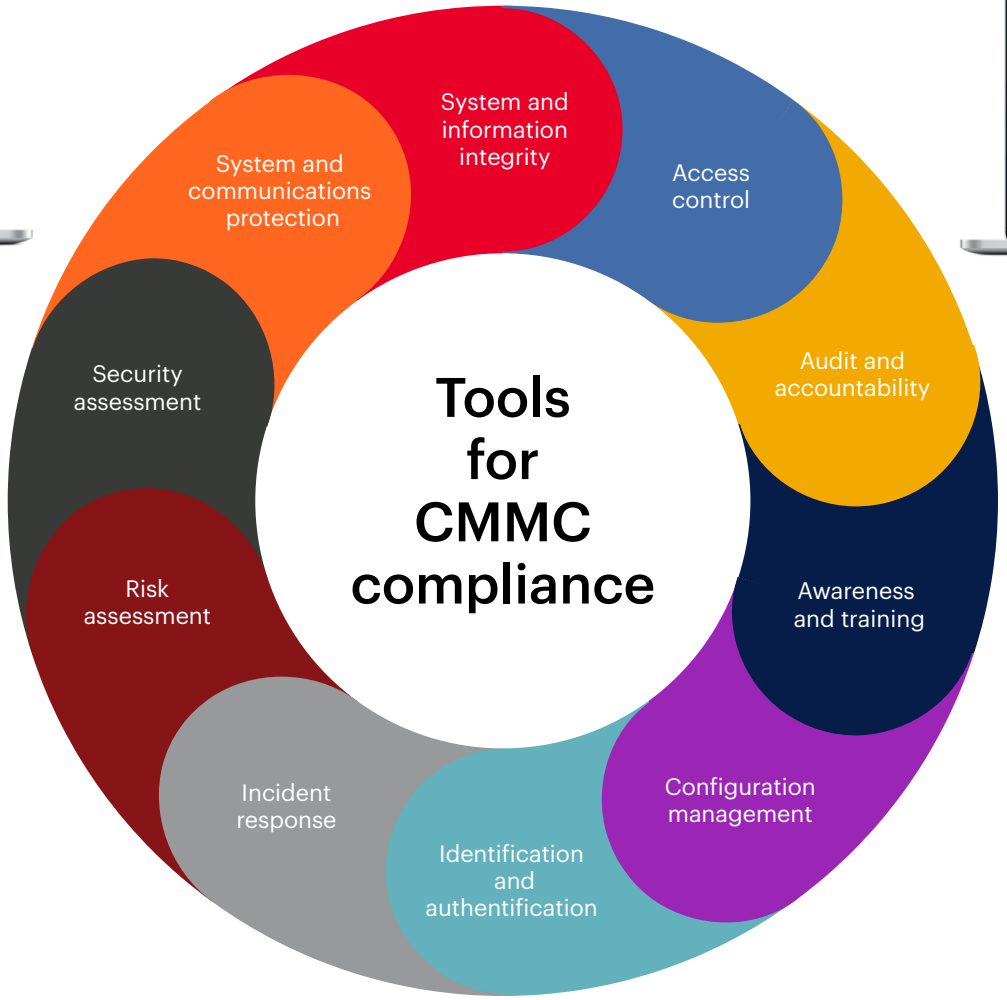
Keysight CyPerf



Keysight IoT Security Assessment

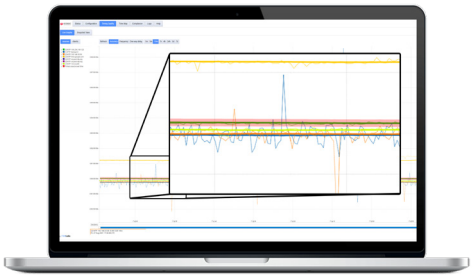


Keysight BreakingPoint

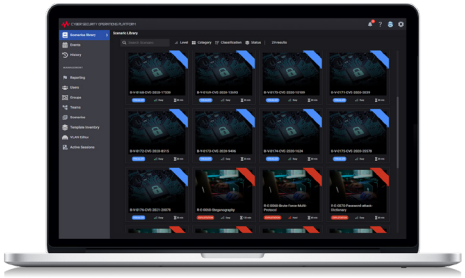


Keysight Application and Threat Intelligence

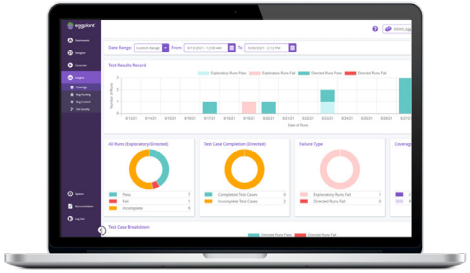
Keysight Network Packet Brokers and Taps



Keysight TimeKeeper



Keysight Cyber Range



Keysight Eggplant

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.