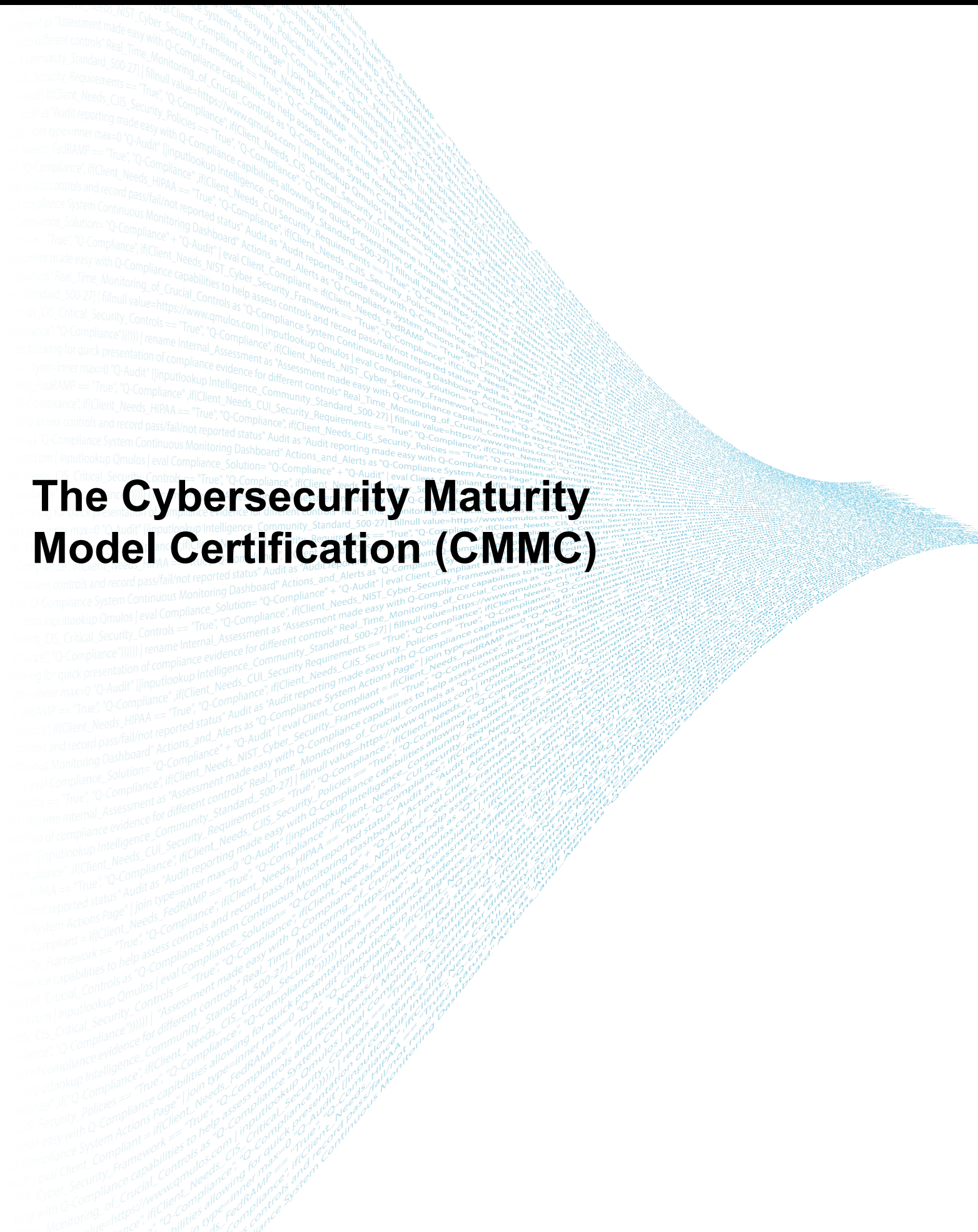
The Cybersecurity Maturity Model Certification (CMMC)



Product Brief

CMMC: Q-Compliance

REAL-TIME CON-MON RISK MANAGEMENT FOR THE DEFENSE INDUSTRIAL BASE

The Cybersecurity Maturity Model Certification (CMMC) v2 framework, published on November 17, 2021 introduced new standards of accountability and security in the defense industry. CMMC is designed to build upon pre-existing standards like the Defense Federal Acquisition Regulation Supplement (DFARS) and National Institute of Standards and Technology (NIST) frameworks. Unlike DFARS, however, CMMC is strictly enforced and requires defense contractors to be audited and certified by a third-party auditor (3PAO). Adhering to CMMC requirements allows your organization to bid on and hopefully win DoD contracts. But without the certification, good luck!

An estimated 200,000-350,000 contractors, including custodial companies, bookkeepers, caterers, and small IT firms, will need to hold a CMMC certification. The new model follows the Pentagon's assessment that one of their greatest cybersecurity risks comes from the second and third-tier DoD contractors. As such, when it comes to awarding contracts, cybersecurity will now be the "fourth critical measurement," along with quality, cost, and schedule.

CMMC is broken into 3 maturity levels covering 14 domains, with levels building on each other. For instance, to achieve a Level 2 certification you must also implement the Level 1 requirements. Fortunately, if you were adhering to the standards set forth in DFARS or NIST 800-171, you likely meet the requirements of Level 1. However, meeting the higher level requirements in time may be a challenge depending on your organizational maturity. Luckily, our flagship solution, Q- Compliance, assesses your environment, shows the failing controls, and provides a step-by-step process to get to the next level. It also stores the needed evidence, files, links, and human activity to show auditors you're ready to win that next contract.

Before hiring an outside C3PAO, you should do a self-assessment to ensure you are meeting Level 1. Level 1 consists of 17 controls and parallels the DFAR 52.204-21 requirements, which all federal contractors must meet. It represents basic cyber hygiene and the minimum standards any contractor should have already deployed. While Qmulos is not a C3PAO, we provide the software to self-assess against the CMMC controls with our out-of-the-box CMMC dashboard, proving to the C3PAO of your choice, where you stand.

The CMMC v2 framework measures the maturity of an organization's cybersecurity practices covering several domains. The domains are broad categories of critical security functions such as Access Control, Identification and Authentication, Incident Response, etc. The categories should sound familiar, as they come directly from the NIST 800-53 control families. These domains are further broken down into 110+ best practices (controls).

splunk> POWERED

Looming CMMC Compliance Deadlines

- **FY 2022** — The DoD will increase the number of its contracts containing CMMC requirements to approximately 75 – this will likely impact about 7500 defense contractors that will need to achieve CMMC certification.
- **FY 2023** — The number of contracts with CMMC requirements will increase to 250, affecting approximately 25,000 contractors.
- **FY 2024** — The contract total will jump to 325, which will impact about 32,500 defense department contracting entities.
- **FY 2025** — By the time we reach the quarter-century milepost, there will be about 479 DoD contracts requiring approximately 47,905 defense contractors to achieve CMMC Certification.
- **FY 2026** — By October 2025, the DoD plans to include a CMMC Certification requirement in all of its future contracts.

At Qmulos, we pride ourselves on simplifying compliance.

As native Splunk powered solutions, Q-Compliance and Q-Audit solve the problem of adhering to CMMC and other security standards. Q-Compliance and Q-Audit are purpose-built to streamline and automate complex cybersecurity requirements like CMMC. We further enhanced Q-Compliance with features specifically for CMMC, building the product upon the same standards and best practices used in this new security model. Similarly, Q-Audit provides prescriptive, out-of-the-box auditing capabilities to meet ICS 500-27. The ICS 500-27 standard will satisfy many of the practice requirements from the CMMC Audit and Accountability domain.

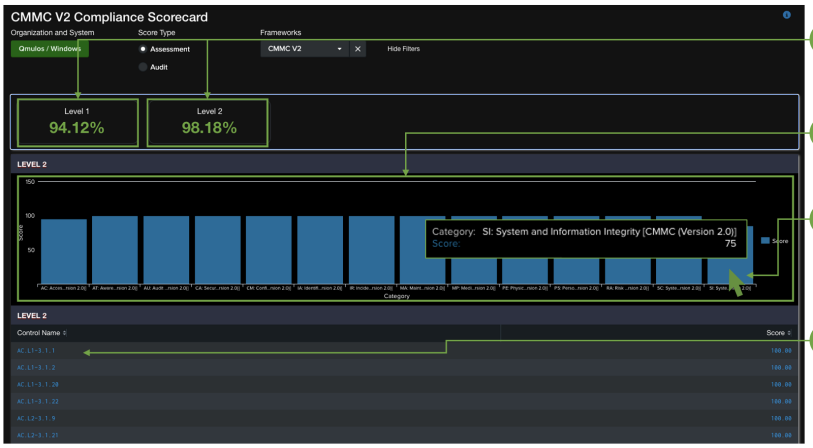
Additionally, we align specific security controls with the domains, capabilities, and practices from CMMC. We leverage real-time log and event data from Splunk to automate the assessment and scoring of your organization's practices against the CMMC maturity levels. Furthermore, we codified industry best practices into the application workflow, enabling your organization to institutionalize and optimize processes to improve your cyber posture for CMMC, NIST 800-53, HIPAA, SOX, CJIS, NERC CIP, and many other standards. Not to mention protect sensitive information such as Federal Contract Information and Controlled Unclassified Information.

Using Q-Compliance's out-of-the-box CMMC dashboard, users can track how an organization and its systems score against each of the five levels, and identify what needs to be done to meet the next level's requirements. The dashboard provides the ability to quickly drill into specific domains to view compliance against the capabilities, practices and processes set forth in the model, and also drill into individual controls to see the specific systems, events, and assets that are non-compliant.

Both Q-Compliance and Q-Audit give the user the ability to upload policies, procedures and file evidence, as well as automatically log human activity. Qmulos' software suite keeps evidence needed for audits all in one place, efficiently organizing critical information for the C3PAO of your choice.

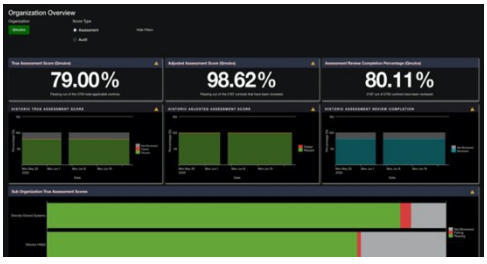
While CMMC may seem daunting, it doesn't have to be. Winning or renewing your DoD contract is important, and with the best practices codified into our solutions, no matter what your maturity level, Splunk knowledge, or technical experience, Qmulos has you and your team covered!

CMMC Dashboard to Score Against Maturity Levels



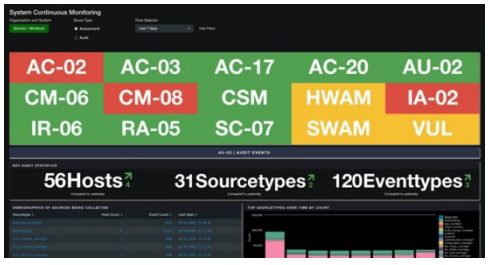
Note: Level 3 scores will be created when DoD defines the Level 3 requirements

ExecutiveView



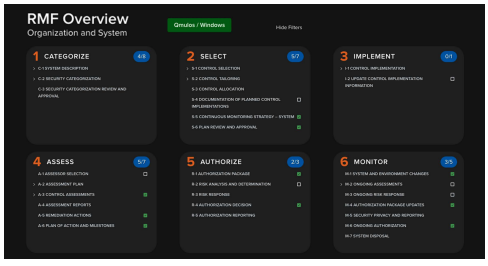
- Compliance and risk postures
- Organization & system views
- View status across different compliance frameworks

Control Monitoring



- Real-time risk and compliance visibility
- Single pane of glass for all evidence and artifacts
- Workflows for time and event-based assessments

Native RMF Features



- Support for all RMF steps
- Overlay management
- Organization, system, and asset management
- Control tailoring
- Assessment automation