qmulos®

CMMC Made Simple

The Q-Compliance User's Guide to CMMC

Put Q-Compliance to Work for CMMC

You have invested in a new generation of compliance that is automated, real-time, and converges the functions of compliance, risk, and security. This core business strategy - and mindset - is necessary to evolve legacy compliance and risk management practices into business-aligned, integrated, modern enterprise and cybersecurity risk management programs.
Q-Compliance solutions help keep organizations compliant with major compliance frameworks such as NIST 800-171, NIST 800-53, ICS 500-27, SOX, HIPAA, FedRAMP, and PCI DSS. ***Now you can add CMMC to the list.***

CMMC: Similar Standards, A New Way of Thinking

CMMC is the first of many future requirements that will force federal contractors to transform compliance from its decades-old role as a historical reporting function into a modern tool of continuous enterprise risk management. The CMMC (Cybersecurity Maturity Model Certification) program's intent is to ensure better cybersecurity posture visibility across the defense industrial base (DIB). The objective is to protect Controlled Unclassified Information (CUI) that is shared by the Department of Defense (DoD) with its contractors and subcontractors from being breached by cybercriminals and our nation's adversaries.

It is anticipated that CMMC 2.0 will be codified into law in the first half of 2023, with its newly defined cybersecurity compliance requirements being gradually applied to DoD contracts. The good news is that you're ahead of the game since you already use Q-Compliance.

Future-Proofs Against Evolving CMMC Framework Updates

Q-Compliance for CMMC is future-proofed against the evolution of the CMMC standard, as well as against internal technology changes. Built on a flexible, scalable, and data- agnostic platform, Q-Compliance for CMMC enables rapid updates as compliance requirements change, mitigating the need for re-work and manual intervention.

It also easily accommodates internal technology updates, keeping organizations protected and prepared for the ever-changing landscape of compliance standards, cybersecurity threats, and technology.

Q-Compliance:

- Compliance agility: an organization's ability to rapidly adjust to shifting compliance requirements as they emerge
- Compliance readiness: the ability to respond to audit requests in a timely manner
- Compliance confidence: the ability to ensure traceability and veracity of reported compliance information

CMMC is Coming and You're Perfectly Positioned to be Ahead of the Game

We can help you get ahead with a joint upfront effort to onboard the required data sources. Once this one-time implementation commitment is made, it solves so many issues in perpetuity because the data will automatically flow in for years.

Depending on the compliance frameworks you are already following you may already be capturing all of the data needed to meet the technical controls of CMMC. If not, it's a straightforward addition to your Q-Compliance license and the Qmulos team can switch on the CMMC dashboard for your organization.

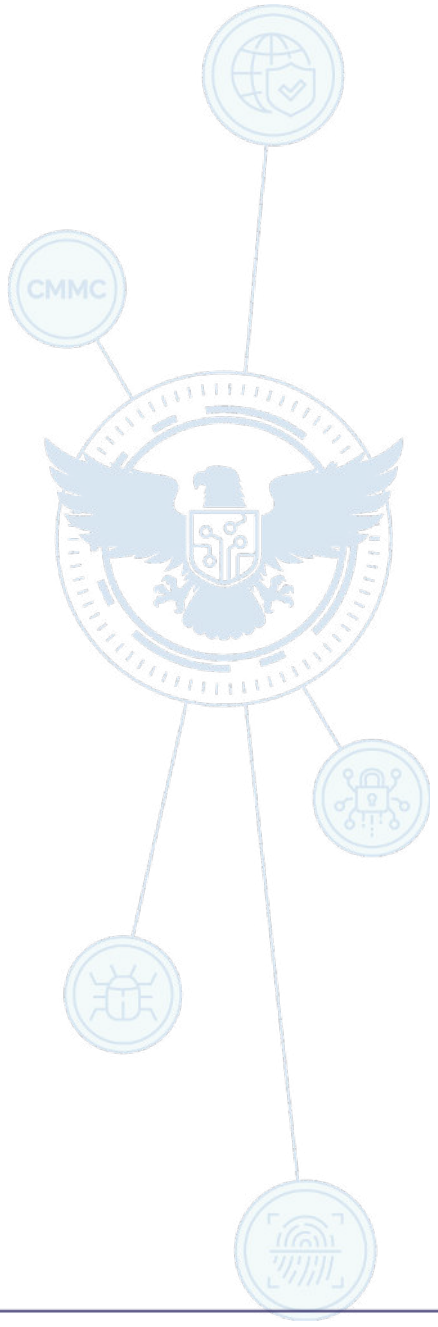
Q-Compliance for CMMC is the only always-on cybersecurity compliance solution in-market today. Its automated technical evidence collection, assessment, and reporting delivers Converged Continuous Compliance™, streamlining your ability to meet current and future requirements and strengthening the overall cybersecurity posture of the business. It is on the same compliance platform used by the DoD, federal agencies, and large commercial organizations, enables enterprises to confidently accelerate and demonstrate compliance by leveraging big-data analytics and user-friendly visualizations.

What Makes CMMC Unique?

CMMC is about private sector players having real skin in the national security game. Once CMMC is fully implemented, organizations that cannot achieve, maintain, and credibly demonstrate compliance will find themselves unable to compete for or deliver under DoD contracts.

Any control deficiencies identified during audits will no longer be allowed to persist indefinitely under extended mitigation timelines; concrete deadlines for closing known risk gaps will be established and enforced. When firms begin to see their P&L impacted by compliance posture, it makes security real – and that's the point.

Q-Compliance for CMMC accelerates the ability of DIB organizations to achieve and demonstrate CMMC compliance through big-data analytics and user-friendly visualizations. Its real-time data ingestion and assessment help organizations achieve accurate, traceable, and up-to-the-minute compliance, protecting against revenue loss or non-compliance delays. With Q-Compliance for CMMC, users can trace evidence down to a single data point, ensuring complete compliance confidence even while the framework of CMMC continues to evolve.



Q-Compliance:

- Enables leadership confidence to sign off on compliance and audit reports
- Ensures you can demonstrate completion of any remediation plan related to POAM's 180-day implementation audit
- Supports a trusted data-driven process

For more information on how Q-Compliance can help automate CMMC compliance and other frameworks, please visit our CMMC page or reach us at sales@qmulos.com.

About Qmulos

Qmulos is a pioneering next-gen compliance, security and risk management automation provider, delivering the innovative power of converged, continuous compliance through its flagship Q-Compliance and Q-Audit technology platforms. Qmulos enables organizations to achieve high compliance confidence while delivering a powerful and engaging compliance experience across all functions and phases of the enterprise compliance lifecycle. Government and industry leaders in the public and private sectors use Qmulos' solutions to ensure the highest levels of cybersecurity.

qmulos.com

qmulos