qmulos®

WHITE PAPER

# DoD Demands Diligence

## In an Era of Intense Accountability, Cybersecurity Compliance Is the New Competitive Advantage

Legacy compliance management practices leave enterprises unable to competently deal with emerging mandates. 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 cybersecurity risk management.

## Executive Summary

The intent of the CMMC (Cybersecurity Maturity Model Certification) program is to ensure better visibility of the cybersecurity posture across the defense industrial base (DIB), creating a unified model for validating compliance as part of the DoD acquisitions process. 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. In late 2021, CMMC was introduced to incorporate a set of cybersecurity requirements into DoD programs and provide increased assurance that contractors and subcontractors are meeting these requirements. It is anticipated that CMMC 2.0 will be codified into law, with its newly defined cybersecurity compliance requirements being gradually applied to DoD contracts, and with a target of FY 2026 for the inclusion of CMMC 2.0 provisions in every defense contract.

Simply put, CMMC 2.0 is about private sector players having a significant commitment to national security. Once CMMC 2.0 is fully implemented, organizations that cannot achieve, maintain, and credibly demonstrate compliance will find themselves unable to work with the DoD, which can put millions, if not billions of dollars in revenue at risk. 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 their compliance posture, it makes an impact – and that's the point.

CMMC 2.0 is not just an updated version of yet another framework or standard. It's about making a serious and concerted effort to shore up the security of confidential national defense data entrusted to the vast network of approximately 300,000 industry partners comprising the defense industrial base. CMMC 2.0 demands more transparency, greater oversight, and real personal accountability for company officials. It also seeks consistency in third-party assessments to ensure compliance claims stand up to scrutiny and reflect true enterprise risk posture. In other words, plausible deniability is out, and personal accountability is in.

The answer is converged continuous compliance that not only enables compliance agility, but simplifies meeting current and ongoing compliance requirements comprising the Defense Industrial Base (DIB).

# How Should DIB Organizations Be Thinking About CMMC 2.0 and Compliance?

Traditionally, compliance for federal contractors could be described as attempts at proactive risk management in the form of ATOs (Authority to Operate), and reactive risk posture reporting in the form of assessments and outside audits, or "compliance after the fact."

ATOs were designed to ensure security of systems and software as they entered the federal or contractor IT ecosystems. Assessments and audits, conducted before system turn-up or on a periodic basis during its lifecycle, were meant to validate security controls on the "as-designed" basis; primarily a view of the intended system state. However, nothing was built into the process to ensure continuous efficacy of the controls between these periodic activities.

The problem with this model is the inherent compliance lag built into these heavily manual, siloed, and paper-based processes. In a typical triennial audit cycle, failed controls could remain undetected for up to three years or even longer, depending on the accuracy of the reauthorization process and the quality of the control data, largely collected and interpreted through manual means.

The ostensible "answer" to these inherent limitations has come in the form of "provisional ATOs" and "POAMs" – in essence, temporary waivers that effectively allowed unmitigated risk to be carried on the books for extended periods, kicking the proverbial risk-can down the road.

> Bottom line: Federal cyber and IT compliance could be described as one giant paper tiger, a massive resource drain with little to show for it in the way of actual effective security and risk management.

Despite efforts from Nation Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and Office of Management and Budget (OMB), federal compliance has largely remained a periodic "snapshot in time," a static, paper-based effort. Although the concepts of continuous monitoring exist in NISTs Risk Management Framework (RMF), DHS's Continuous Diagnostics and Mitigation (CDM) Program, and various OMB Memorandum such as OMB Memo 21-31, the implementation of these programs has fallen well short of their intent.




It bears mentioning that no definitive count of defense contractors subject to CMMC exists. Estimates range from as low as 80,000 firms to 300,000. This lack of visibility further highlights the urgent need for the DoD to gain a better understanding of the risk posture across the defense industrial base.

## Large System Integrators Will Make Decisive Moves to Remove Threat from Their Supply Chain

The whole point of CMMC is to shore up risks within the defense supply chain. System integrators (SI) are only as secure as their weakest link, so if a contractor is using legacy compliance practices, trying to apply them to CMMC 2.0 will not just hurt, it will likely siphon their revenue stream. Some vendors may already be compliant with CMMC 2.0 requirements, but do not have an easy way of knowing or reporting. Relying – and trusting – on objective, technical control data versus subjective opinion is the answer.

The largest DIB contractors have an immense supply chain themselves, all of which must be CMMC-compliant, upstream and downstream, depending on the type of information it holds. Figuring out the applicability is half the battle. Ensuring compliance is the other half. Managing this consistently, confidently, and continuously across the supply ecosystem is an enormous challenge. The outcomes will be:

- Supply chain teams will be forced to ensure all suppliers are up to speed. They will need to see factual data, visible in real-time, to solve for CMMC 2.0.
- Companies will have to move quickly as waivers and extensions are going away.
- DIBs begin to recognize their compliance posture as a matter of competitive advantage. They know CMMC 2.0 compliance is fast becoming table stakes for DIB players and want to avoid being outmaneuvered.

## What Should the Evolved DIB Contractor Compliance Model Look Like?

Designing a comprehensive security program, based on an honest and unflinching threat model of your environment, is hard enough – but it's only half the job. Keeping a constant watch over the state of your defensive apparatus, inclusive of people, processes, and technology, is the other half. The goal should be to build it right and keep it running while maintaining full visibility.

Enterprise cybersecurity teams expect to be able to monitor inbound threats in real-time. Why is that not true of the compliance requirements that govern them?
Moving to continuous control monitoring is a rapidly emerging trend driven by real-world experience and regulatory developments alike.

The need for top-down accountability in compliance and risk management – think Sarbanes Oxley (SOX) – is evident in the frequent headlines and lawsuits playing out where security and business leaders alike are being held individually accountable for misreporting of compliance control posture, especially in cases of breaches or whistleblower disclosures like Aerojet Rocketdyne.

Leaders and CISOs have to understand and manage confidence risk across their enterprise compliance programs and promote ongoing compliance requirements that, if not met, will have implications for their teams and themselves. Too many "complacent" organizations exhibit a desire to move quickly to check boxes required by individual compliance frameworks, but not do the hard work of ongoing oversight that can be automated by technology. This exposes organizations to significant risk and increases compliance costs. This can easily be changed by leveraging existing data analytics to run real-time risk mitigation for converged, continuous compliance.

As private sector firms comprising the Defense Industrial Base come further into scope of the new CMMC 2.0, the trend towards proactive and continuous control monitoring will extend to other commercial enterprises as well. The federal IT ecosystem is already rolling out such protocols with EO14028 and M-21-31.

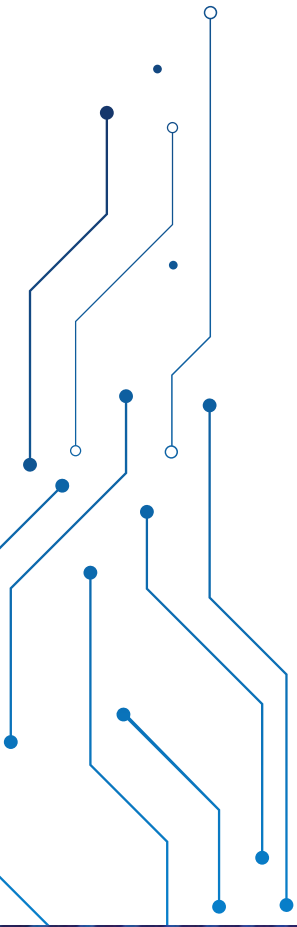
## What Can Defense Contractors Do to Get Ahead, Yet Not Be Stuck?

Compliance requirements will only get more stringent as cybersecurity grows in importance and threats continue to grow. Organizations must take an honest look at their compliance management practices – not just the last compliance report, but the organization, the people, the processes, and the technology employed to manage all that effort. Then, ask a simple question: How much of our compliance reporting is informed by actual data (i.e. collected directly from IT assets and security controls) as opposed to opinion (i.e. manual reports collected from system owners and interpreted by risk analysts to the best of their knowledge and experience)? And, how much of our data is real-time?

If you don't know, or recognize that your answer is not satisfactory, it's a good indicator that your compliance management practices are not mature enough to deliver the credible, reliable, and timely data required for CMMC 2.0, or other future requirements.

Now is the time to embrace data-driven convergence as a path to trustworthy risk, security, and compliance management maturity. Technology exists that not only automates compliance, but puts it at the center of supporting your security posture in a proactive way. Transforming compliance from a siloed activity to a driver of increased security through technology will deliver benefits today and well into the future.

## CMMC 2.0 – DIBs Will Be Asked to Represent True Risk with Facts, Not Opinion



The lightbulb moment for DIB contractors is when they realize that their entire risk model is predicated on opinion. Contractors need to exercise true enterprise risk management (ERM) – business risk and compliance risk are converging, just as lawsuits around misrepresenting true risk are rising. Coincidence? No.

The next era of cybersecurity across the DIB contractor base requires total visibility to risk, meaning upstream and downstream transparency. The days of placing blame elsewhere or relying on a supplier to send their latest self-assessment questionnaire are over. As was seen with Aerojet Rocketdyne, hiding behind disclaimers is no longer going to work. Major players like Lockheed and Raytheon will require policies that ensure supplier compliance and traceability, and shift away from periodic general 3rd party risk management practices.

Ultimately, all of these shifts are about protecting government information that is entrusted to the private sector, not about compliance opinion, but about compliance facts, backed by real-time data.

Modern Compliance Operations means:

- Deriving real value from your data and reporting on it with confidence
- The ability to login to your supplier's Qmulos instance to generate factual, data-driven reports in real-time
- Automating compliance, not shuffling paper faster, to assure major suppliers that what they declare to the DoD is sound
- Saying goodbye to the old-school scorecard, which is an opinion statement, not a system.

This is what it means to have compliance agility, and it's the only way to survive the DoD supply chain vendor scrutiny that lies ahead.

"EVERYONE IS RELYING ON "THE GUY BEHIND THE GUY." THE CISO HAS TO PULL THE RISK OUT"

DoD should focus their third-party auditors who are being certified as we speak (IG equivalents) on auditing controls that make a difference to security – namely technical controls. If not, they will just create huge costs for contractors trying to comply without achieving the actual benefits of complying. Contractors trying to comply should take every opportunity to proactively tailor and prioritize the real-time monitoring and ongoing mitigation of controls that are important to security (tech controls) to avoid bloated costs spent on paperwork and realize true security value."

IGOR VOLOVICH

Vice President, Compliance Strategy,
Qmulos

## What Can Contractors Do – Today – to Better Comply with Federal Cybersecurity Frameworks Like CMMC 2.0?

The practice of compliance management is heavily reliant upon the collection of evidence and control artifacts. Historically, and even today, most organizations expend significant manual effort to collect, validate, organize, analyze, and report compliance control artifacts. Despite major technological advances, far too many compliance management organizations find themselves conducting "data calls", highly manual tasks to collect information about controls from administrators, operators, and system owners. The churn and overhead are simply inexcusable, yet most enterprises simply accept it as a cost of doing business. Compounding the problem are the armies of service providers whose entire business model depends on keeping compliance management a manual effort.

The good news is, the data informing the enterprise about its compliance controls and overall security and risk posture already exists, with millions of data points produced by each component of an organization's IT infrastructure every second. The only thing stopping enterprises from leveraging that data to make truly informed and timely risk management decisions is often the same old culprit: compliance complacency, the "we've always done it this way" syndrome.

The concept of convergence recognizes a simple truth: there is no distinction between compliance data, risk data, and security data; it's all data. We just need to make sense of it through the proper lens: compliance, risk, or security. Naturally, this requires shifting from the perception of compliance as a siloed cost of doing business and an unwelcome overhead expense, and transforming it into a powerful source to timely, accurate, and trusted risk intelligence.

Convergence is impossible without data-driven automation. Luckily, the technology to make it possible is available today.

# Qmulos Q-Compliance Remedies Supply Chain Vulnerabilities

Qmulos doesn't just deliver point solutions; its Q-Compliance solution transforms compliance in the very best sense to meet every compliance requirement with simple adjustments to the data collected and analyzed.

With Q-Compliance, DIB contractors can now automate their self-assessments across most compliance frameworks long before a third party shows up. The solution provides contractors with a dashboard of data-backed evidence on-demand to be able to show, not just assert, that benchmarks are being met. Put simply, Qmulos' Q-Compliance automates the hard part. The source of technical evidence no longer matters, it can be swapped all day long. It is "firewall data" and the models automatically know what to analyze and report on.

If a DIB contractor has SOX and wants CMMC, meeting the new compliance standards is a minimal investment if the data has already been ingested. It is just a different lens that allows movement from one framework to the next, no configuration updating is needed. Just add the controls that make the data visible.

> Qmulos can assist you with a full suite of compliance requirements, no matter what framework or custom standard you adhere to.
>
> If you are interested in a Q-Compliance demo, please email sales@qmulos.com and one of our cyber compliance and risk management automation experts will be in touch.

**contact us**

## 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