Cyber **security**

PREPARING FOR CYBERSECURITY MATURITY MODEL CERTIFICATION



THREAT READY

LRQA

Your Risk Management Advantage

PREPARING FOR CYBERSECURITY MATURITY MODEL CERTIFICATION

For many Department of War (DoW) contractors and subcontractors, the arrival of Cybersecurity Maturity Model Certification (CMMC) presents an opportunity to build on existing cybersecurity investments. Organisations that have already worked to implement NIST SP 800-171r2 and its 110 controls to protect Controlled Unclassified Information (CUI) are particularly well positioned to achieve CMMC certification quickly and demonstrate their commitment to safeguarding sensitive data at an even higher DoW recognised standard.

It's important to understand that CMMC is not a new or separate cybersecurity framework that replaces NIST SP 800-171r2. Instead, CMMC is a verification model designed to assess and certify an organisation's implementation of NIST SP 800-171r2.

In essence:

- CMMC Level 1 focuses on basic safeguarding of Federal Contract Information (FCI) using a subset of 17 practices derived from FAR 52.204-21.
- CMMC Level 2 directly evaluates the full implementation of the 110 security requirements in NIST SP 800-171r2 for organisations that handle Controlled Unclassified Information (CUI) derived from DFARS 252.204-7012.

Rather than requiring contractors to adopt an entirely new set of practices, CMMC serves as the DoW's mechanism to:

- Confirm that NIST SP 800-171r2 controls are not only documented in policies and plans, but are fully and consistently implemented across people, processes, and technology.
- Provide third-party or self-attestation assurance that the supply chain is protecting CUI at the required level.

This means organisations that have already achieved strong NIST SP 800-171r2 compliance, particularly those with mature System Security Plans (SSPs), have closed out their Plans of Action and Milestones (POA&Ms), and documented evidence of ongoing control effectiveness, are already well positioned for CMMC Level 2.

With a focused gap assessment against CMMC's practice and objective requirements, targeted evidence collection, and where needed third-party assessment coordination, your organisation can efficiently transition from NIST SP 800-171r2 compliance to CMMC certification leveraging existing investments while gaining formal, DoW recognised validation of your cybersecurity posture.

As a global certification and cybersecurity leader with accredited assessors and consultants in both North America and Europe, LRQA is uniquely positioned to support U.S. defense contractors and their international subsidiaries, as well as European-based organisations in the Defense Industrial Base, through every phase of CMMC preparation and certification.



WHAT IS THE CYBERSECURITY MATURITY MODEL CERTIFICATION?

CMMC is a cybersecurity framework designed by the DoW to assess, enhance, and verify the cybersecurity readiness of organisations throughout the Defence Industrial Base (DIB). It ensures that contractors and subcontractors can effectively protect FCI and CUI when performing DoW contracts.

CMMC is structured around 14 security domains derived from NIST standards. Each domain consists of specific capabilities that represent the key functions needed to achieve maturity in that area. For example, the Incident Response domain includes capabilities such as Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity.

These capabilities are supported by detailed practices and objectives that demonstrate both technical implementation and understanding. Organisations pursuing certification are assessed depending on the sensitivity of the information they handle and the associated contract requirements.

A significant portion of CMMC practices align directly with the security requirements outlined in NIST SP 800-171r2, which has long served as the baseline for protecting CUI in non-federal systems. While there is substantial overlap making the transition more manageable for organisations already compliant with NIST 800-171r2, CMMC introduces important advancements:

- A tiered model that evaluates not only whether controls are implemented but also how consistently and effectively they are managed and optimised over time.
- Third-party or self-assessment and certification requirements depending on level, providing the DoW with greater assurance and visibility into supply chain cybersecurity.
- Streamlined requirements in CMMC that reduce complexity while maintaining strong protection of sensitive information.

CMMC builds upon and strengthens the foundation established by NIST 800-171r2, offering a more comprehensive, verifiable, and scalable approach to safeguarding the DoW supply chain. It reflects DoW's ongoing commitment to promoting a resilient and cyber-secure defence ecosystem in partnership with industry.



DEVELOPING A STRATEGIC ACTION PLAN FOR CMMC COMPLIANCE

Achieving CMMC represents a valuable opportunity to strengthen your organisation's cybersecurity posture while positioning it for continued success in the Defence Industrial Base. By approaching compliance through a structured, milestone driven framework, the process becomes manageable, predictable, and highly rewarding.

STEP 1: DETERMINE YOUR TARGET CMMC LEVEL

Begin by identifying the CMMC level your organisation needs to achieve based on the sensitivity of the information you handle, Federal Contract Information or Controlled Unclassified Information based on contracts. Clearly defining this target early provides a focused roadmap for all subsequent efforts.

STEP 2: CONDUCT A COMPREHENSIVE GAP ASSESSMENT

With your target level established, review the specific practices and processes required across all 14 domains. Compare your current policies, procedures, and technical controls against these requirements.

- If your organisation has previously aligned with NIST SP 800-171r2, leverage existing documentation, self-assessments, and third-party audit results as an accelerated starting point.
- Document where current controls fully meet, partially meet, or do not yet meet CMMC requirements.

STEP 3: REMEDIATE IDENTIFIED GAPS

Prioritise and implement necessary updates to policies, procedures, and technical controls. Communicate changes effectively to relevant personnel and provide training where needed to ensure proper adoption.

STEP 4: VALIDATE EFFECTIVENESS THROUGH INTERNAL ASSESSMENT

Once updates are in place, perform thorough internal testing and evidence collection to confirm that controls are not only designed correctly but are also operating effectively in practice. Document results, address any findings, and refine controls as required.

STEP 5: EMBRACE CONTINUOUS MONITORING AND IMPROVEMENT

CMMC is built on the principle of ongoing maturity. Establish regular review cycles, incorporate lessons learned, and maintain clear evidence of processes. These practices form the foundation of long-term resilience and compliance.

THE STRATEGIC ADVANTAGE OF ACTING NOW

Proactively pursuing CMMC compliance delivers immediate and lasting benefits:

- Significantly enhanced protection of sensitive information
- Stronger overall cybersecurity resilience
- A clear competitive edge when bidding on DoW contracts

Even if external factors shift final implementation timelines, every step you take toward CMMC alignment directly strengthens your organisation's security program and positions you as a trusted, forward-thinking partner in the defense supply chain. By starting today with a clear, phased approach, your organisation can move confidently from preparation to certification and become not just compliant, but distinctly more secure and competitive.

LRQA'S CMMC SERVICES

With Certified CMMC Professionals (CCPs) and Certified CMMC Assessors (CCAs) teams operating across the United States and Europe, LRQA delivers consistent, high-quality CMMC advisory and assessment services regardless of where your CUI environment or team is physically located.

CUI DISCOVERY ASSESSMENT

Before investing significant amounts of time and resources into CMMC compliance, every defence contractor needs to answer one critical question: Where is your CUI located, who has access, and how is it currently protected?

A professional CUI Discovery engagement delivers immediate clarity and helps prevent costly mistakes:

- Accurately define your scope to identify all systems, endpoints, cloud environments, and shared drives that fall within your target CMMC level
- Avoid over-spending by preventing applying Level 2 controls to systems that are outside the scope of your CUI environment.
- Eliminate surprises by uncovering unnecessary IT environments, unauthorised cloud storage, and legacy repositories holding CUI that would otherwise derail your assessment.
- Accelerate your timeline with a verified CUI boundary and data flow maps in hand, gap assessments and SSP development become faster and far more accurate.

Companies that skip discovery routinely overspend and face major rework when the C3PAO finds undocumented CUI assets at work. Starting with a focused CUI Discovery is the smartest, fastest way to predictable and cost-effective CMMC certification.

CMMC LEVEL 1 ADVISORY SERVICES

Even at Level 1, DoW contracts now require formal self-attestation and getting it wrong can mean immediate loss of eligibility.

An LRQA CMMC Level 1 Advisory Services gives you certainty in weeks, not months:

- Rapid identification of all in-scope people, assets, and processes that handle FCI.
- Expert guided documentation of your 17 basic cyber hygiene practices and procedures.
- Independent evaluation of evidence to confirm every practice is performed exactly as required.
- A complete assessment ready self-attestation package, including PoA&M close-out if needed, signed and uploaded to SPRS with confidence

Many contractors assume Level 1 is easy and self-attest prematurely, only to fail contract awards when the government questions their evidence. LRQA's structured consultation eliminates guesswork, prevents costly false starts, and delivers a fully documented, defensible Level 1 attestation in as little as 2–4 weeks.

Walk away with proof of compliance today, protect current contracts, and build the foundation for seamless progression to Level 2 whenever you're ready.

CMMC LEVEL 2 ADVISORY SERVICES

CMMC Level 2 is no longer a future requirement, it is the new minimum for most DoW contracts handling CUI. A failed or delayed Level 2 certification can lock you out of millions in opportunities.

LRQA CMMC Level 2 Advisory Services deliver clarity, speed, and certainty:

- Precise scoping of your CUI environment and enclave boundaries
- Expert-led gap assessment against all 110 NIST 800-171r2 controls
- Full development/review of your SSP, asset inventory, data flow diagrams, and POA&M.
- Evidence collection guidance and pre-assessment validation to ensure every control meets the adequate and sufficient requirements
- A complete, C3PAO-ready package plus prioritised remediation roadmap

Companies that go it alone routinely underestimate scope, miss critical evidence, or face 6-12 months of rework after formal assessment. LRQA's proven consultation cuts months off your timeline, dramatically reduces findings, and positions you for a smooth, successful C3PAO assessment often achieving certification in a single pass.

Get Level 2 right the first time. Protect your pipeline, win more awards, and turn compliance into a competitive advantage.

CMMC LEVEL 2 CYBERSECURITY CONSULTANCY

Achieving CMMC Level 2 certification is just the beginning. Certification expires in three years, and the DoW expects continuous compliance, any lapse risks contract loss during annual affirmations or the next C3PAO reassessment.

LRQA's Level 2 Cybersecurity Consultancy keeps you certified, confident, and assessment ready year-round:

- Ongoing evidence collection and control monitoring across all 110 NIST 800-171r2 controls
- Scheduled incident response tabletop exercises and lessons-learned integration
- Annual risk assessments and Operational Plan of Action management
- Continuous SSP and asset inventory updates as your environment evolves
- Pre-reassessment health check and mock assessment to eliminate surprises
- Additional specialised cybersecurity services to include penetration testing, vulnerability scanning, incident response, digital forensics, and tabletop exercises.

Organisations without sustained support routinely drift out of compliance, face major findings at reassessment, or scramble at the last minute. With LRQA as your embedded compliance partner, you maintain processes, pass reassessments effortlessly, and free your team to focus on mission-critical work. Stay certified. Stay competitive. Turn CMMC from a one-time project into a permanent business advantage with LRQA Advisory Services and Cybersecurity Consultancy.

CMMC MODEL

	MODEL	ASSESSMENT
LEVEL 3	**134 REQUIREMENTS** (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172	• DIBCAC certification assessment every 3 years • Annual affirmation
LEVEL 2	**110 REQUIREMENTS** aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual affirmation
LEVEL 1	**15 REQUIREMENTS** aligned with FAR 52.204-21	• Annual self assessment • Annual affirmation

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage