

Redspin's CMMC Gap Assessment

A Tailored CMMC Gap Assessment for Compliance, Decreased Risk, and Peace of Mind

If you're a prime or subcontractor within the Defense Industrial Base (DIB), a CMMC gap assessment is a critical first step to ensure you meet cybersecurity requirements validated by the Department of Defense's (DoD) new Cybersecurity Maturity Model Certification (CMMC) standards to gain and maintain DoD contracts and secure our nation's data.

Redspin's CMMC gap assessment goes beyond a checkbox exercise and uncovers potential vulnerabilities and weaknesses in your current cybersecurity practices to help you make a clear, actionable, timely plan to achieve your desired CMMC maturity level before a formal assessment.

The Challenge

A traditional check-the-box CMMC gap assessment doesn't address underlying security risks that could compromise sensitive data, disrupt operations, and cost you contracts. It creates a false illusion that, at a high level, you won't miss essential compliance requirements. However, cursory reviews can ultimately lead to non-compliance. When the assessment focuses only on documentation, you can miss critical vulnerabilities. Additionally, poorly defined Controlled Unclassified Information (CUI) boundaries or inadequately detailed policy documentation create scope creep and other issues during a formal assessment.

The Solution

A CMMC gap assessment is a proactive readiness approach that ensures your organization effectively protects sensitive information like FCI and CUI against evolving cyber threats. Redspin's gap assessment goes beyond superficial compliance. It helps your organization build a robust cybersecurity foundation for your unique environment. By identifying and addressing security weaknesses in your current security profile and comparing them to your target CMMC profile, your organization can confidently expect to ace a formal CMMC assessment and ultimately secure contract requirements, accept contract awards, and win new business.

Our Experience



The First

Redspin is the first authorized CMMC 3rd Party Assessment Organization (C3PAO).



Experienced Certified Assessors

Our team of CCAs bring more than two decades of knowledge on CMMC requirements.



Cyber AB Collaboration

We maintain close relationships with the Cyber AB.



DoD Expertise

Our consultants bring experience from both sides of the DoD contracting process.



Pioneers in CMMC

We have led CMMC since its inception, drive industry thought leadership, and serve as active Standards Council members.



What makes a Redspin Gap Assessment different?

We take the time to understand your current state...

Our in-depth assessments go beyond surface-level checks, thoroughly analyzing your practices and controls, not just your documentation, to reveal cybersecurity strengths and weaknesses.

- Our experienced assessors, including former DoD contracting CISOs, CIOs, and military veterans, understand the unique challenges DIB organizations face.
- Identifies areas where your organization meets or falls short of CMMC requirements and provides practical, actionable compliance and security guidance.
- Ensures open communication and a collaborative approach throughout the assessment process.

We help you develop a strategic plan...

With a clear understanding of your cybersecurity posture, we help you develop an actionable roadmap to successful CMMC certification.

- Ensures open communication throughout the process, creating a strategic partnership for your entire CMMC compliance journey.
- Works collaboratively with your teams to identify risks, vulnerabilities, and areas needing additional focus.
- Provides tailored recommendations to proactively address gaps, ensuring your program meets CMMC requirements.
- Supports your ongoing compliance and helps mature your practices over time.

You avoid costly disruptions...

Non-compliance with CMMC can lead to significant disruptions, including loss of DoD contracts, financial penalties, and reputational damage.

- Identifies and addresses compliance gaps, ensuring you meet necessary standards to avoid costly disruptions and maintain eligibility to be awarded DoD contracts

You strengthen your cybersecurity posture...

Redspin's assessments extend beyond compliance, enhancing your overall cybersecurity framework.

- Identifies and mitigates potential vulnerabilities, strengthening your defenses against cyberattacks.
- Protects sensitive government data and safeguards your business from evolving threats.

Demonstrate Commitment...

Redspin's assessments provide tangible evidence of your proactive efforts to protect sensitive government information.

- Builds trust and confidence with current and potential clients
- Sets you apart from competitors that may take a more reactive security approach
- Establishes a robust cybersecurity framework to protect critical information and serve the DIB effectively