Helping DoD Contractors Prepare For — and Ace — CMMC Requirements

The Department of Defense (DoD) requires all contractors and subcontractors that store, process, and/or transmit Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) to be compliant with CMMC certification requirements. Compliance begins at Level 1 and spans to Level 3 for more complex and highly sensitive CUI.

While some organizations can self-attest to compliance at Level 1 and, in limited cases, at Level 2, most will require a formal CMMC assessment to verify compliance at Levels 2 and 3.

Redspin's expert guidance helps contractors and subcontractors throughout the CMMC lifecycle, beginning with a gap assessment and continuing through readiness remediation planning to scoping, enclave build-out, policy development, employee training, preparation for the formal CMMC assessment, and remediation support. Redspin's CMMC experts work closely with clients to tailor solutions to their specific needs and ensure they meet rigorous CMMC requirements.

Redspin Knows What it Takes to Prepare for and Pass CMMC.

- First Authorized CMMC Third-Party Assessment Organization (C3PAO) and first to be re-certified.
- Unparalleled experience and insight into CMMC development and evolution
- Deep understanding of NIST 800-171, CMMC, assessment processes, and compliance requirements
- Client-tailored, end-to-end services to meet each organization's unique needs and challenges

What are Redspin Consulting and Readiness Services?

Redspin's Consulting and Readiness Services help organizations achieve and maintain compliance with the Cybersecurity Maturity Model Certification (CMMC) framework — from initial CMMC readiness assessments to remediation strategies, all the way through preparedness for a formal CMMC certification.

The Challenge

There's a worldwide shortage of skilled cybersecurity and compliance professionals. For DoD contractors that are fortunate enough to attract and retain these employees, many just don't have the in-house support, resources, or CMMC-specific subject matter experts to help them implement required controls and documentation to ensure compliance.

It's hard for these teams to understand exactly what CMMC is and what it means for their business. That's further compounded because there isn't a one-size-fits-all CMMC implementation approach for every contractor. There are many organization-specific factors that directly impact CMMC scoping. They must be able to understand if they have FCI or CUI, where it is, and how it's used. This is different for every contractor.

Additionally, many DoD contractors are overwhelmed with the seemingly daunting task of implementing the 110 NIST security controls required for Level 2 compliance. That's even harder for contractors at Level 3, who must successfully implement, document, and demonstrate all those controls plus additional security standards that address advanced persistent threats (APTs).

Many contractors don't have the knowledge, time, or skilled personnel to properly document their compliance efforts, which is a crucial step for CMMC compliance.

The Solution

Redspin's consulting services help DoD contractors overcome these challenges, wherever they are. They provide expert guidance on CMMC requirements and compliance processes, including:

- ✓ Security control and program gap assessments
- ✓ Developing compliance roadmaps
- ✓ Creating and maintaining CMMC-compliant documentation
- ✓ Ongoing CMMC compliance maintenance

Redspin's Consulting and Readiness Partnerships

Redspin helps DoD contractors and subcontractors confidently meet CMMC requirements to secure — and maintain — contracts to work within the DIB.

Tailored gap assessments

Go beyond inefficient checkbox processes to understand potential security gaps in your current cyber practices to reach your intended CMCC maturity level.

- Get a thorough review of your current practices and policies to see where you fall short of framework requirements
- Assess severity and potential impact to prioritize remediation
- Create a roadmap to address gaps, including necessary steps, resources, and timelines to achieve compliance
- Get actionable recommendations for improvement, including technical solutions, policy changes, and employee training

Supply chain vetting and compliance

As a CMMC contractor, your subcontractors that access FCI and CUI must also be CMMC compliant. Get help vetting supply chain vendors and proactively ensuring compliance to decrease the risk of a breach of compliance penalty, like contract loss.

- Assess vendors' cybersecurity posture to determine if they meet CMMC requirements, like reviewing security policies, controls, and documentation
- Get expert guidance on selecting CMMC-compliant vendors
- Get support to help vendors with remediation to address CMMC compliance gaps

Actionable compliance roadmaps

Develop prioritized implementation plans to reach CMMC maturity, including roles, responsibilities, and timelines.

- Define clear metrics and milestones to track progress and ensure effective remediation
- Align CMMC compliance with existing processes and systems to streamline implementation and minimize disruptions
- Get guided remediation and support to quickly and effectively navigate challenges
- Develop processes for continuous security control monitoring and improvement

Compliant documentation and assessment prep

Develop a documentation framework for organizing and managing all compliance documentation, ensuring it is accessible and auditable.

- Use pre-built templates and guidance to develop and implement essential CMMC policies and procedures
- Automate artifact collection
- Map documentation to CMMC controls
- Prepare for certification with clear documentation

Why Redspin?

As the nation's first authorized C3PAO, Redspin has been at the forefront of CMMC since day one. The company's expert-led CCP and CCA training courses cut through CMMC's complexity, giving you in-depth knowledge, hands-on experience, and guidance to pass your exams and keep pace with the changing CMMC landscape.

- Understand complex CMMC requirements
- Implement NIST-based security controls like multi- factor authentication, user access and identity management, and incident response
- Develop comprehensive documentation for compliance
- Ace your CMCC assessment and achieve certification for your desired CMMC compliance level