GUIDEPOINT® SECURITY

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) COMPLIANCE SERVICES

Close CMMC Compliance Gaps to Better Protect FCI and CUI

Organizations that store, process, transmit or generate Controlled Unclassified Information (CUI) for the U.S. Department of War (DoW) are required to achieve, maintain and attest to CMMC compliance.

Enhance CMMC compliance efforts with GuidePoint Security CMMC services. Our certified consultants understand how to apply CMMC controls to each environment. Our experts meet organizations where they are. We help them understand the FCI and CUI in their care. Together, we identify issues, define remediation plans, and close compliance gaps so our clients achieve certification and compliance.

Ensure CMMC Compliance

Commercial organizations doing business (directly or indirectly) with the U.S. Department of War (DoW) are required to hold a Cybersecurity Maturity Model Certification (CMMC) as a condition of contract award. GuidePoint Security CMMC services help organizations determine if CMMC applies and identify and remediate gaps to achieve compliance.

Since 2018, the DoW has required contractors to be NIST SP 800-171-compliant based on a self-service review. However, many prime and sub-contractors handling Federal Contract Information (FCI) and/or Controlled Unclassified Information (CUI) still cannot fully account for FCI and/or CUI they store, process, transmit, or generate, or have access to as a subcontractor. Now, the DoW can discretionally require entities to achieve CMMC compliance as a condition of contract award, effectively adding a third-party certification and attestation layer to a previously self-attestation scenario. Organizations impacted include:

- ✓ Those who process, store or transmit FCI or CUI
- ✓ Those who provide security protections for any assets processing, storing or transmitting FCI or CUI
- ✓ Those who provide or manage platform infrastructure, applications or storage services for those organizations (e.g., ESPs, CSPs)

GuidePoint experts can help identify and document all FCI and CUI data flows, determine CMMC in-scope environment and implement scope reduction as needed, build asset inventories and maintenance processes, and perform gap assessments against the in-scope environment.
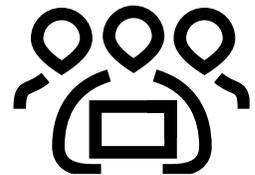
Stronger Together. Securing What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and U.S. intelligence agencies.

THE CYBER AB
CMMC CERTIFICATION
REGISTERED PRACTITIONER ORGANIZATION
RPO

Achieve CMMC Compliance Faster

As a CMMC Registered Provider Organization (RPO), GuidePoint Security works with organizations across the U.S. to improve their CMMC compliance efforts. Our Registered Practitioner (RP), Registered Practitioner Advanced (RPA), and CMMC Certified Professional (CCP) consultants understand the nuances of CMMC. We help organizations understand both their environment and how to best leverage CMMC in line with organizational needs. GuidePoint services include:

CMMC Scoping Exercise: Nail down the specific people, processes, and technologies to which CMMC applies.

- ⊘ Identify and document information systems (e.g., people, technology, facilities, external service providers) that process, store, or transmit FCI and CUI or are otherwise in scope as defined by 32 CFR Part 170.

CMMC Gap Assessment: Gain visibility into current compliance status and required addressable areas to prepare for certification.

- ⊘ Identify your in-scope environment and applicable required controls.
- ⊘ Validate controls to ensure coverage of all CMMC Assessment Objectives.
- ⊘ Define remediation activities required to obtain a CMMC certification.
- ⊘ CMMC Compliance Program Implementation Support: Build and operate a program that facilitates ongoing compliance and attestation.
- ⊘ Develop and/or revise standard-specific documentation required for compliance.
- ⊘ Educate personnel on roles and responsibilities and demonstrate them.
- ⊘ Participate in the formal audit on your side of the table as a liaison and advocate.

Advisory Services: GuidePoint experts are available as on-demand extensions of your team as consultants, staff augmentation, and/or Compliance Program Implementation Support (CPIS) to achieve and maintain CMMC certification.

CMMC Levels

| Entities that process, store, or transmit FCI and not CUI | **Level 1** | **Level 2** Self Assessment | Entities that process, store, or transmit **non-DoW** CUI |
| Entities that process, store, or transmit **DoW** CUI | **Level 2** Certification Assessment | **Level 3** | Entities that process, store, or transmit CUI identified by DoW as representing a higher risk than Level 2 |

The CMMC Level required will be specified by the DoW in the contract.

Why GuidePoint Security

When cyber threats hit, you want the best on your side. GuidePoint Security designs, deploys, and delivers tailored cybersecurity solutions that drive real results. We integrate solutions across any environment — faster, smarter, and with less risk to strengthen your defenses. Accelerate your business with confidence – and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow.