

SHIELDCompliance Product Suite - CMMC



INTENT

CTI's SHIELDCompliance assists customers with achieving cybersecurity regulatory or standards requirements to meet the Cybersecurity Maturity Model Certification (CMMC). Our SHIELDCompliance assessments aid organizations analyze their IT security environment for control strength and effectiveness and compare their overall posture to requirements outlined in the relevant cybersecurity regulation(s) or standard(s). The three tiers of assessments that comprise the SHIELDCompliance suite provide varying degrees of review and documentation suitable to diverse needs and budgets. Recommendations for new controls and configuration guidance for existing controls are provided to help address compliance gaps.

COMPONENTS

The following graphic illustrates the various assessments available as part of CTI's SHIELDCompliance. These services range from concise one to three-day engagements to detailed multi-week assessments.

SHIELDCompliance CMMC - Express

CTI's SHIELDCompliance - CMMC Express is designed to provide organizations with a gap analysis versus the CMMC requirements that match their relevant level. The assessment evaluates compliance with the CMMC through interviews of key personnel, high-level data gathering, and inputting findings into a SaaS application to assist with management of CMMC compliance.

SHIELDCompliance CMMC - Core

CTI's SHIELDCompliance - CMMC Core is a more extensive engagement that builds on the elements of SHIELDCompliance - CMMC - Express engagement. Additional services include performing a Risk Assessment, developing policies, plans, and procedures to meet the applicable customer CMMC requirements.

SHIELDCompliance CMMC - Pro

CTI's SHIELDCompliance - CMMC Pro is CTI's most comprehensive offering that builds on the elements of SHIELDCompliance - CMMC - Core engagement. Additional services include ongoing maintenance of CMMC SaaS application, cybersecurity policies, plans, and procedures to meet the applicable customer CMMC requirements.

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

BENEFITS

1) Improve Knowledge and Understanding of Security Risks

This program will establish or improve employee awareness of security risks, which will lead to expedited identification of security gaps, better informed security-related decision-making, and the input required for development of remediation roadmap(s).

2) Reduces Organization’s Financial, Legal, and Reputational Liability

The regular presence of a dedicated IT security professional improves the organization’s overall security posture and will position the organization to proactively address vulnerabilities before they are exploited by an attacker, reducing the likelihood of an attack, and any resulting financial, legal, or reputational damages.

3) Security Guidance

CTI consultants will provide guidance for cybersecurity program management, security control acquisition, and assist with configuration of any current controls that do not satisfy industry best practice recommendations. Remediation steps will be provided to bring device configuration(s) into compliance.

4) Certification Preparedness

Preparedness for CMMC certification by identifying gaps and recommended remediation for addressing gaps in your organization’s security posture versus the CMMC requirements.

- Increased effectiveness in planning and budgeting for annual security efforts.
- Increased internal awareness of security risks results in expedited identification of security gaps, better-informed security-related decision-making, and the input required for development of a remediation roadmap.
- Communicating the results of a SHIELDCompliance CMMC assessment and the resulting security remediation roadmap to executive stakeholders’ garners sponsorship and support from upper management, demonstrating organizational due diligence in handling employee and / or customer sensitive data.

CMMC MATURITY LEVEL

The CMMC Framework requires a systematic approach to certification mapped to three organizational maturity levels: Expert, Advanced, Foundational.

