Xacta® for CMMC

Helping Defense Contractors Protect the Sensitive Unclassified Information in Their Custody

Overview

Cybersecurity Maturity Model Certification (CMMC) is a unifying standard developed by the U.S. Department of Defense. It is intended to ensure that members of the Defense Industrial Base (DIB) are applying sound cybersecurity and risk management practices in order to protect sensitive unclassified information.

Unlike earlier standards for DIB information assurance, CMMC requires a CMMC Third-party Assessor Organization (C3PAO) to verify the cybersecurity maturation level of all DoD contractors that handle Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the DoD supply chain.

CMMC has been effective since November 30, 2020 with a phased rollout through September 30, 2025. DoD has continually stressed that DIB contractors should begin preparing now to ensure their competitive edge when the time comes to bid on a CMMC-required contract.

Xacta for CMMC: Cyber Risk Management for the Defense Industrial Base

In response, Telos® has developed the Xacta 360® CMMC offering to support contractors and vendors within the DIB that require or need to prepare for certification and assessment by a C3PAO.

Because CMMC is an evolving standard, our offering enables you to assess the maturity level required today as well as build a roadmap to the maturity level of tomorrow. After identifying your current implementation, the application walks you through a self-assessment of the CMMC level you intend to achieve. Xacta includes the official CMMC requirements as well as their assessment procedures as defined by the Office of the Secretary of Defense. Telos maintains this content, along with associated risk and compliance frameworks or standards (such as NIST SP 800-171) within our Xacta platform, and makes updates available when changes or additions occur.

With Xacta's CMMC offering, you can quickly and easily:

- Automate the process of preparing for a CMMC assessment
- Manage compliance with NIST SP 800-171 and CMMC within the same project
- Ascertain the scope of your CMMC assessment for all associated CAGE codes
- Manage CMMC requirements across multiple DoD contracts
- Identify the data supply chain for FCI and CUI data

- Utilize Xacta's control inheritance capabilities while implementing the required CMMC controls for your expected maturity level
- Conduct CMMC self-assessments and organize artifacts demonstrating compliance for an efficient C3PAO audit
- Create and maintain CMMC System Security Plan and NIST SP 800-171 Scorecard
- Generate a Supplier Performance Risk System (SPRS) Score using the NIST SP 800-171 DoD Assessment Methodology.
- Log and track cyber incidents for DIBNET reporting
- Monitor and maintain your certified environment for easier recertification every three years

How does the Xacta CMMC offering work?

As is true with all other Xacta 360 offerings, Xacta for CMMC works much like tax preparation software, helping the user navigate the end-to-end process.

Users are presented with a series of input screens that collect and organize all of the data needed for the CMMC assessment. These screens are organized in a logical manner and prompt the user to answer questions and input the data needed to ensure all identified gaps and deficiencies are eliminated *before* the C3PAO walks through the door.

Xacta also generates related documentation (SSP, security assessment summary, and CMMC scorecard) as a byproduct of the process. You do not have to generate these documents from scratch at the end of the process. Xacta does this for you based on your inputs.

How will the Xacta CMMC offering benefit me?

- You will not have to rely on email and spreadsheets to manage the process. Xacta centralizes CMMC compliance activities, underlying data, assessments, and evidence.
- The offering can reduce the cybersecurity and information assurance expertise required to complete CMMC preparatory activities.
- This simplification of the process also reduces your dependency on expensive, hard-to-find cybersecurity and IA personnel.
- Xacta for CMMC automatically generates evidentiary documents when you need them.
- The offering ensures a smooth assessment process when the C3PAO arrives.
- Xacta allows you to efficiently manage and maintain your CMMC certification over time by utilizing automated control periodicity.

Will the Xacta CMMC offering save me time?

Xacta 360 will save you weeks of time interpreting and implementing the CMMC process. Smaller organizations with few cybersecurity and IA resources will realize a dramatic benefit.

The application will save you days and perhaps weeks of time (depending on the size of your environment) establishing your IT asset and cloud resource inventory affected by FCI and CUI.

The document generation process is completely automated. Xacta generates all documents, based on user data inputs. This function also saves weeks of time.

Why Telos and Xacta 360?

Xacta was first launched in 2000 to help accelerate risk management and regulatory compliance activities through automation. Our goal from the very beginning has been to simplify and automate the underlying functions of those activities as much as possible. Today, Xacta is the recognized leader in federal government framework automation solutions for the enterprise.

With this offering, we have applied our vast risk management expertise to address a similar problem: empowering DIB contractors with awareness and management of the CMMC certification process. There is no better source for preparing for your CMMC certification than Telos and Xacta.

Please contact us to learn more about how Xacta can simplify and automate the CMMC certification process for your organization.

Telos Corporation

1-800-70-TELOS (800-708-3567)

info@telos.com

telos.com/xacta-cmmc