Prevalent

Cybersecurity Maturity Model Certification (CMMC)

Conduct standardized assessments for all 17 capability domains and all 5 certifications under the CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a single standard for all US Department of Defense (DoD) acquisitions and meant to ensure that the entire US national defense supply chain is secure and resilient. CMMC requires that each of the more than 300,000 DoD contractors achieve third-party certification.

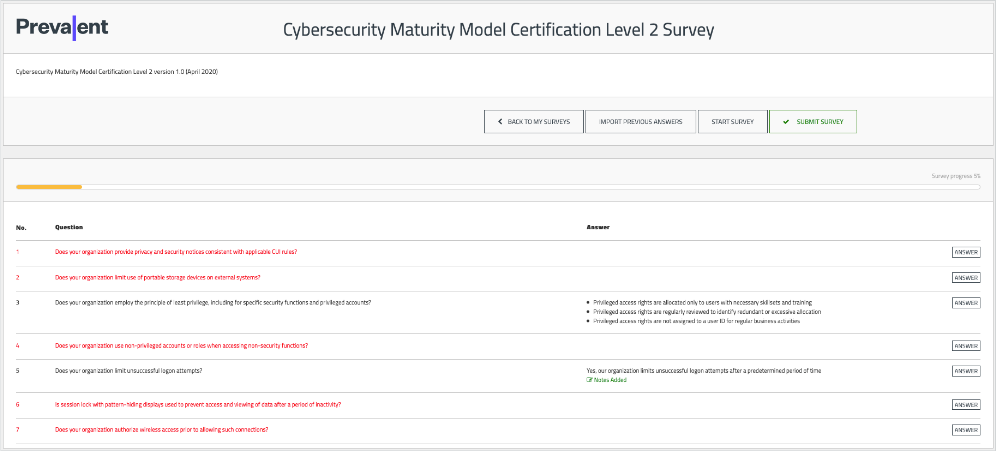
Conduct CMMC Assessments with Prevalent

The Prevalent Third-Party Risk Management Platform provides a single solution for certified third-party audit organizations (C3PAOs) and DoD contractors to assess, report on and remediate risks across all CMMC domains and practice areas.

Questionnaires are available in the Prevalent platform for each certification level based on established guidelines in the Federal Acquisition Regulation (FAR) Clause 52.204-21, Security Requirements for Controlled Unclassified Information (CUI) from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, per the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204.7012.

Key Benefits

- Simplifies and accelerates risk identification and audit reporting with a single platform for all CMMC questionnaire levels
- Improves visibility with clear scoring and compliance status against accepted DoD standards
- Ensures auditors and contractors use the most current questionnaires with automatic updates



Cybersecurity Maturity Model Certification Level 2 Survey

Cybersecurity Maturity Model Certification Level 2 version 1.0 (April 2020)

Survey progress 5%

No.	Question	Answer	
1	Does your organization provide privacy and security notices consistent with applicable CUI rules?		ANSWER
2	Does your organization limit use of portable storage devices on external systems?		ANSWER
3	Does your organization employ the principle of least privilege, including for specific security functions and privileged accounts?	• Privileged access rights are allocated only to users with necessary skillsets and training • Privileged access rights are regularly reviewed to identify redundant or excessive allocation • Privileged access rights are not assigned to a user ID for regular business activities	ANSWER
4	Does your organization use non-privileged accounts or roles when accessing non-security functions?		ANSWER
5	Does your organization limit unsuccessful logon attempts?	Yes, our organization limits unsuccessful logon attempts after a predetermined period of time	ANSWER
6	Is session lock with pattern-hiding displays used to prevent access and viewing of data after a period of inactivity?		ANSWER
7	Does your organization authorize wireless access prior to allowing such connections?		ANSWER

The Prevalent platform provides questionnaires addressing every CMMC domain and practice area with easy-to-use audit reporting.

Learn more at **www.prevalent.net**

Key Features for Auditors

Perform CMMC Assessments for All 5 Levels

CMMC certified auditors can use the Prevalent Third-Party Risk Management Platform with all five levels of CMMC controls questionnaires included. With this access, certified auditors can:

- Invite clients into the Prevalent platform to complete standardized control assessments in an easy-to-use, secure tenant
- Automate chasing reminders to clients to reduce the time required to complete assessments
- Centralize supporting documents submitted as evidence of the presence of controls
- Produce a single risk register based on client responses
- Issue remediation recommendations for failed controls

Key Features for DoD Contractors

Perform CMMC Level 1 Self-Assessments

DoD contractors can use the Prevalent Third-Party Risk Management Platform to conduct a Level 1 pre-assessment prior to the formal audit. With this access, DoD contractors can:

- Assess against the 17 controls required to measure Level 1 compliance
- Upload documentation and evidence to support answers to questions
- Gain visibility into current compliance status
- Leverage built-in remediation guidance to address shortcomings prior to your formal audit
- Produce compliance reports for auditors

TPRM Platform

Prevalent delivers the industry's only purpose-built, unified third-party risk management platform.

Assess

Automate the process of collecting, analyzing, remediating and reporting on vendor evidence.

Share

Partner with vendors through shared repositories of validated questionnaires with supporting documents.

Monitor

Make better risk-based decisions with technical insight into threats, breaches and network health, combined with a strategic view of business risks.

Consult

Plan, optimize and mature your TPRM program with professional services, or take advantage of managed services options.

> "We have risk reporting on time when we need to report to the authorities. Consistent reporting metrics is another key benefit."
>
> - S&P 500 Financial Services Company

Learn more at **www.prevalent.net**