Prevalent

# Cybersecurity Maturity Model Certification (CMMC)

**Conduct standardized assessments for CMMC certification**

The Cybersecurity Maturity Model Certification (CMMC) is a single standard for all US Department of Defense (DoD) acquisitions and is 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 at one of three levels, depending on whether they handle controlled unclassified information (CUI).

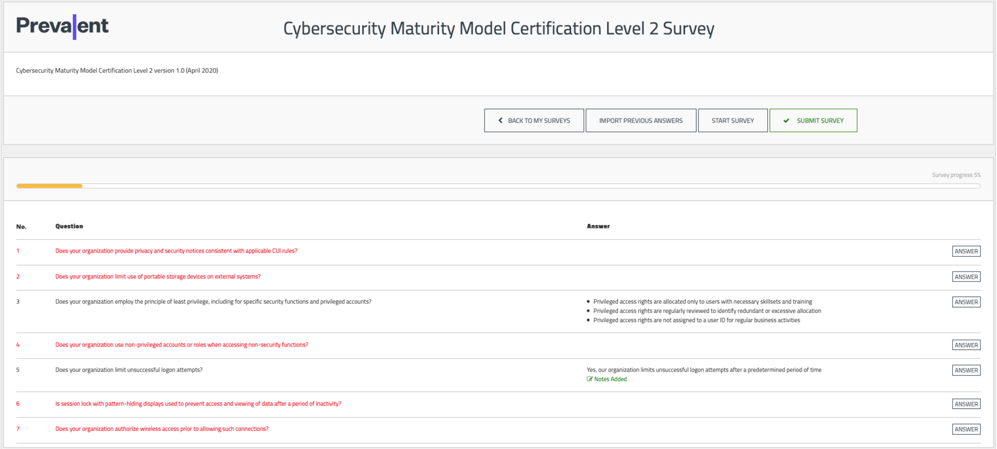
## Conduct CMMC Assessments with Prevalent

The Prevalent Third-Party Risk Management Platform provides a single solution for suppliers and certified third-party audit organizations (C3PAOs) to assess, report on and remediate risks across all CMMC domains and practice areas. The Prevalent Platform addresses each CMMC certification level with questionnaires derived from:

- basic safeguarding requirements for Federal Contract Information (FCI) specified in *Federal Acquisition Regulation (FAR) Clause 52.204-21*
- security requirements for controlled unclassified information (CUI) specified in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2* per *Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012*
- additional controls from *NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*

## 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<br>• Privileged access rights are regularly reviewed to identify redundant or excessive allocation<br>• 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<br>Notes Added | 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 Level 2 CMMC Assessments

CMMC certified auditors can use the Prevalent Third-Party Risk Management Platform to:

- Invite suppliers into the Prevalent platform to complete their standardized Level 2 control assessment in an easy-to-use, secure tenant
- Automate chasing reminders to reduce the time required to complete assessments
- Centralize supporting documents submitted as evidence of the presence of controls
- View a single register of risks raised depending on how the supplier responds to the questions
- Issue remediation recommendations for failed controls
- Deliver customized reporting on the current level of compliance, demonstrating the risk-reducing impact of the application of future control

** Information on Level 3 will be released by the US DoD at a later date and will contain a subset of the security requirements specified in NIST SP 800-172.*

## Key Features for Suppliers

### Perform Level 1 and Level 2 Self-Assessments

DoD contractors can use the Prevalent 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
- Assess against the 110 controls required to measure Level 2 compliance
- Upload documentation and evidence to support answers to questions
- Gain visibility into current compliance status
- Leverage built-in remediation guidance to address shortcomings with third parties
- Produce reporting to measure compliance for auditors

## About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

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