FORTRA™

SOLUTION BRIEF (TRIPWIRE)

CMMC Compliance with Tripwire

How Tripwire Enterprise Keeps CUI Safe for the DoD

The U.S. Department of Defense (DoD) is implementing the Cybersecurity Maturity Model Certification (CMMC) program to standardize the level of cybersecurity implemented throughout its 300,000 suppliers. In practice, this means that every member of the Defense Industrial Base (DIB) will be required to pass an audit in order to win DoD contracts. Compliance for a small number of contracts began in 2020, and phases in to the entire DIB over the next five years.

How the CMMC Is Structured

The way CMMC is structured is fairly straightforward. At the highest levels are 17 domains. These are functional areas such as access control or physical security. Within each domain, there are processes, capabilities and best practices.

Processes can be thought of as the regularly occurring events or plans needed to maintain security. Processes are usually stated very generally, such as: "Establish, maintain and resource a plan that includes Access Control." These processes are broadly stated to allow for the variances that naturally exist in different organizations.

Capabilities are more functional. They describe a specific action that needs to be taken or a goal that must be achieved. One example is: "Perform auditing."

Practices are a group of specific actions. Taken collectively, they allow an organization to create a capability. An example practice would be: "Control posted or processed on publicly accessible information systems." This is one of the 24 practices that make up the access control capability.

Who Must Comply and What Will it Cost?

Bid solicitations will indicate whether a contract requires compliance with CMMC. As the CMMC Audit Bureau (the body responsible for certifying auditors) ramps up the auditing infrastructure, the number of contracts subject to CMMC will increase. By 2026, all new contracts are expected to include CMMC compliance[2].

While a bidder and its subcontractors will be required to demonstrate compliance prior to the bid being awarded, bidders will not be required to be compliant in order to make a bid. The winning bidder will be able to expense certain costs of compliance to help mitigate the impact of CMMC on small suppliers.

HIGHLIGHTS

According to the U.S. Department of Defense, "The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.[1]"

Fortra's Tripwire® Enterprise gives you out-of-the-box compliance testing for the most demanding portions of CMMC (Levels 3–5).

Fortra's Tripwire® Enterprise offers out-of-the-box support for many of the CMMC requirements for Level 3–5 compliance. The data it generates can be used to demonstrate compliance to meet auditors' requirements.

CMMC Levels

CMMC is designed to scale based on the sensitivity of the data that is handled by a contractor. As the data becomes more sensitive, the number and difficulty of practices required increases. Because of this, CMMC is organized into five levels. For example, at Level 1, a contractor is only required to comply with 17 practices, whereas a Level 5 contractor must comply with 171 practices (the 15 practices of Level 5, plus all of the lower level practices).

Also, the level of cybersecurity maturity attained by contractors must increase with the sensitivity of the data handled. At Level 1, contractors must demonstrate that they have changed the default passwords on wireless access points, but they don't have to have written policies or controls that monitor the access points' passwords.

As the CMMC level increases, contractors are expected to operationalize processes. At the highest CMMC levels, contractors are expected to actively tune their cybersecurity tools and processes to respond to a changing threat landscape. The image below depicts this expectation of increasing maturity.

Tripwire Enterprise in a CMMC Deployment

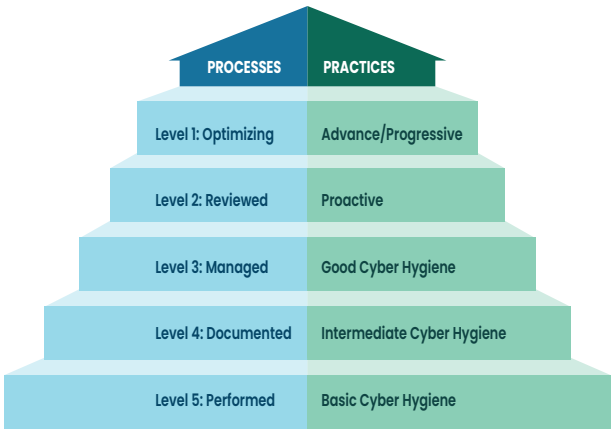
Tripwire Enterprise's role in CMMC is to monitor the network for compliance to CMMC requirements and to provide the evidence that auditors can use to confirm compliance. Specifically, it inspects devices on the network and verifies that practices have been implemented and are being properly maintained.

The Reporting Challenge

Tripwire Enterprise eliminates the reporting challenge of CMMC by creating reports that demonstrate compliance to auditors. For example, if network device passwords are supposed to be changed every three months, Tripwire regularly scans them and reports if their passwords were indeed changed appropriately. If a password has not been changed according to policy, the variance is flagged in the report. A waiver or explanation is then required to explain why the policy was not followed.

The 17 Domains of the CMMC

1. Access Control (AC)
2. Access Management (AM)
3. Awareness and Training (AT)
4. Audit and Accountability (AU)
5. Configuration Management (CM)
6. Identification and Authentication (IA)
7. Incident Response (IR)
8. Maintenance (MA)
9. Media Protection (MP)
10. Personnel Security (PS)
11. Physical Protection (PE)
12. Recovery (RE)
13. Risk Management (RM)
14. Security Assessment (CA)
15. Situational Awareness (SA)
16. Systems and Communications Protection (SC)
17. Systems and Information Integrity (SI)



CMMC model with five levels to measure cybersecurity maturity

Powerful Integrations

Tripwire Enterprise integrates with the following:

- Systems of record, such as ServiceNow, Cherwell, Jira and Remedy
- Tripwire Event Sender, for exporting rich change data to SIEMs like QRadar and Splunk
- Governance, Risk and Compliance (GRC) frameworks

These capabilities are critical for every contractor seeking certification for a number of reasons:

- Planned changes are often documented in a system of record. But proving that only the expected changes occurred is difficult without a tool like Tripwire Enterprise, which confirms expected changes and reports on unexpected ones.
- Organizations often use a SIEM in their security operations center (SOC) as the single pane of glass representing potential security incidents. Tripwire's change data and security data often play a role in identifying and mitigating security incidents.
- GRC tools are often used to consolidate and report on cybersecurity data like that provided by Tripwire Enterprise. Integration shortens the time-to-value provided by the GRC.

One of Tripwire Enterprise's most fundamental capabilities is establishing a secure baseline configuration for your system and tracking all changes against that baseline. That's the core value of file integrity monitoring (FIM) combined with security configuration management (SCM). Tripwire Enterprise ensures the integrity of your files and systems and keeps a record of all changes. It then produces audit-ready reports to make proof of compliance easier.

LEVEL 1 *PERFORMED*

No Processes

- Select processes are documented where required

LEVEL 2 *DOCUMENTED*

Two Processes

- Each practice is documented, including Level 1 practices
- A policy exists that includes all activities

LEVEL 3 *MANAGED*

Three Processes

- Each practice is documented, including lower levels
- A policy exists that covers all activities
- A plan exists, is maintained, and resourced that includes all activities*

LEVEL 4 *REVIEWED*

Four Processes

- Each practice is documented, including lower levels
- A policy exists that covers all activities
- A plan exists that includes all activities
- Activities are reviewed and measured for effectiveness (results of the review is shared with higher-level management)

LEVEL 5 *OPTIMIZING*

Five Processes

- Each practice is documented, including lower levels
- A policy exists that covers all activities
- A plan exists that includes all activities
- Activities are reviewed and measured for effectiveness
- There is a standardized, documented approach across all applicable organizational units

**Planning activities may include mission, goals, project plan, resoucing, training needed, and involvement of relevant stakeholders*

CMMC maturity process progression

SOURCES

1 https://www.acq.osd.mil/cmmc/faq.html
2 https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/
3 https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.