

# Cybersecurity Maturity Model Certification (CMMC) 2.0

white paper

The theft of intellectual property and sensitive information via malicious cyber activity threatens economic and national security. The U.S. government has responded to this threat by establishing CMMC 2.0, a tiered model with required assessments (certification) and implementation through contracts.

## Context for CMMC

The theft of intellectual property and sensitive information from all industrial sectors due to malicious cyber activity threatens economic and national security. The [World Economic Forum](#) estimates that malicious cyber activity incurred a global cost around \$6 trillion in 2021 – this cost is estimated to grow to \$10 trillion in damages by 2025.

The [Center for Strategic and International Studies](#) estimates that the total global cost of cybercrime exceeded \$1 trillion in 2018 . Malicious cyber actors have targeted, and continue to target, the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD).

The DIB sectors consist of over 300,000 companies that contribute toward the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services.

The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security.

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working with industries to enhance the protection of the following types of unclassified information within the supply chain:

- **Federal Contract Information (FCI):**

FCI is information provided by or generated for the U.S. government under contract not intended for public release.

- **Controlled Unclassified Information (CUI):**

CUI is information that requires safeguarding or dissemination controls consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

**The World Economic Forum** estimates that malicious cyber activity incurred a global cost around \$6 trillion in 2021 – this cost is estimated to grow to \$10 trillion in damages by 2025.

Towards this end, the [Office of the Under Secretary of Defense for Acquisition and Sustainment \(OUSD\(A&S\)\)](#) developed the Cybersecurity Maturity Model Certification (CMMC) framework with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB sector.

The original CMMC model measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats. The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, to inputs from the broader community.



# CMMC 1.0

## CMMC is based upon two previous mandates:

- Federal Acquisition Regulation (FAR) Clause 52.204-21 – published May 2016 - contractors are mandated to protect systems with the requisite 15 basic cybersecurity requirements to secure FCI.
- Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 – published October 2016 – all government contractors and subcontractors must comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to secure CUI.

CMMC 1.0 was first introduced in September 2020 by the DoD as an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041). This interim rule established the three basic features of the CMMC framework:

- Tiered model – CMMC offers different levels of compliance that consider the information being handled and security needs.
- Required assessments – Certification of compliance by either third-party assessors or government partners
- Implementation through contracts – contracts issued by the federal government will require CMMC compliance.

The CMMC model adds a certification element to the previous mandates. Certifications serves to verify that cybersecurity processes and practices toward a specific maturity level have been implemented. CMMC certification specifically provides increased assurance to the DoD that a DIB contractor adequately protects CUI throughout the flow of information between company employees, subcontractors, and suppliers.

Three additional regulations were added in [November 2020](#).

- **DFARS 252.204-7019** - Requires contractors and subcontractors to upload their summary level score for their NIST SP 800-171 DoD assessment (Basic, Medium, or High) to the DoD Supplier Performance Risk System (SPRS).
- **DFARS 252.204-7020** – Establishes the right of the government to audit companies; audits will be carried out by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Companies must provide the government with access to their systems and facilities and verify that subcontractors are compliant.
- **DFARS 252.204-7021** – As of October 1, 2025, CMMC will be required by contract award. Prior to this rollout date, the Office of the Undersecretary of Defense for Acquisition & Sustainment [OUSD(A&S)] must approve the inclusion of CMMC in new acquisitions. The level of mandated CMMC certification must be maintained throughout the contract award period.



# CMMC 1.0 Certification Levels

Your company and the business you conduct with the DoD inform the level of CMMC certification required. CMMC 1.0 included 5 levels (levels 2 and 4 were transitional levels to 3 and 5, respectively).

When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for particular divisions or departments, based on where protected information is handled and stored

## **Level 1 – Basic Cyber Hygiene**

Includes basic cybersecurity suitable for small companies having a subset of universally accepted common practices. The processes at this level would include some basic performed cybersecurity practices. This level has 35 security controls that must be implemented successfully.

## **Level 2 – Intermediate Cyber Hygiene**

Includes universally accepted cybersecurity best practices. Practices at this level should be documented, and access to CUI will require multi-factor authentication. This level includes an additional 115 security controls on top of Level 1.

## **Level 3 – Good Cyber Hygiene**

Includes coverage of all NIST SP 800-171 Rev. 1 controls and additional practices beyond the scope of current CUI protection. Processes at this level are maintained, and there is a comprehensive knowledge of cyber assets. This level requires an additional 91 security controls on top of those covered in Levels 1 and 2.

## **Level 4 – Proactive**

Includes advanced and sophisticated cybersecurity practices. The processes at this level are periodically reviewed, properly resourced, and are improved regularly across the enterprise. In addition, the defensive responses operate at high speed and there is a knowledge of all cyber assets. This level has an additional 95 controls on top of the first three levels.

## **Level 5 – Advanced / Progressive**

Includes highly advanced cybersecurity practices. The processes involved at this level include continuous improvement across the enterprise and defensive responses performed at high speed. This level requires an additional 34 controls.





# CMMC 2.0

The interim rule establishing CMMC 1.0 became effective on November 30, 2020, with more than 850 public comments filed in response. These comments highlighted confusion and trepidation around implementation of CMMC, prompting an internal review. This review was carried out in March 2021 by cybersecurity and acquisition leaders within DoD to refine the compliance policy and implementation processes.

Following the internal review, the DoD published an [Advance Notice of Proposed Rulemaking \(ANPRM\)](#) on November 17, 2021. The proposed changes comprise CMMC 2.0 and will take effect after the rulemaking process is completed (anywhere from [9 to 24 months](#) from November 2021).

Rulemaking will be completed within Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Both rules will have a public comment period. CMMC 2.0 has also been submitted to the Office of Management and Budget (OMB); that review will likely be completed in 2023.

In the meantime, all CMMC pilot programs have been suspended, and certification is not required for any contract until rules have been finalized, including a 60-day public comment period prior to the rule taking effect.

However, the DoD is continuing to urge DIB contractors to evaluate their cybersecurity protocols, organize documentation, and generally prepare for CMMC implementation and enforcement in 2026. The DoD has launched [Project Spectrum](#) to support DIB companies in assessing cyber readiness and adopting cybersecurity best practices.

[Gartner](#) estimates that by 2024, 80% of critical infrastructure organizations will migrate from siloed security solutions to hyperconverged solutions that bridge cyber-physical and IT risks.



## Changes from CMMC 1.0 to 2.0

**More Speed and Flexibility** – Allows waivers of CMMC requirements and lets companies create Plans of Action & Milestones to obtain certification under certain circumstances.

**Less Expensive** – Allows all Level 1 (Foundational) and a subset at Level 2 (Advanced) to show compliance through self-assessments.

**Streamlined Requirements** – CMMC 2.0 focuses on the most critical requirements, reducing the model from 5 to 3 compliance levels.

**Use of Widely Accepted Standards** – The model now uses National Institute of Standards and Technology's (NIST) cybersecurity standards and removes CMMC-unique practices.

**More Accountability** – Increases oversight of professional and ethical standards of third-party assessors.

**Reduction of Tiers** - One of the most obvious changes from CMMC 1.0 to 2.0 is the reduction of tiers from 5 levels to 3. This change removes “transitional” certification levels and clarifies the certification requirements for each level.

## CMMC 2.0 Certification Levels

### Level 1 – Foundational:

Matches 15 controls from FAR 52.204-21 “basic” controls to protect FCI. Annual certifications and self-assessments are completed by company leadership. Equivalent to previous Level 1.

### Level 2 – Advanced:

Based upon the old CMMC 1.0 Level 3; lowers the number of required controls to 110 controls in the SP 800-171 Revision. 2 (NIST SP 800171). This eliminates 20 additional CMMC 1.0 Level 3 controls.

CMMC will distinguish between “prioritized” and “nonprioritized” acquisitions based on the sensitivity of CUI. Prioritized acquisitions may handle CUI related to defense systems, whereas nonprioritized acquisitions may include information on military uniforms. Future rulemakings will likely provide greater detail on prioritization.

Prioritized acquisitions will need to be reviewed by a Certified Third-Party Assessor Organization (C3PAO) every three years. Nonprioritized acquisitions will be subject to less scrutiny, requiring only an annual self-assessment and certification.

### Level 3 – Expert:

Replaces Levels 4 and 5 in CMMC 1.0. Acquisitions at the new Level 3 “Expert” level require triennial, government-led assessments. This level also requires compliance with the 110 controls stipulated in the new Level 2 certification as well as NIST's SP 800-172. This level of certification will not be required by most DIB contractors.



# Changes between CMMC 1.0 and 2.0 Levels.

CMMC Model 1.0		
Model	Assessment	Level
<b>171</b> Practices	<b>5</b> Processes	Third-party
<b>156</b> Practices	<b>4</b> Processes	None
<b>130</b> Practices	<b>3</b> Processes	Third-party
<b>72</b> Practices	<b>2</b> Maturity Processes	None
<b>17</b> Practices		Third-party

<b>LEVEL 5</b> Advanced <i>CUI, Critical Programs</i>
<b>LEVEL 4</b> Proactive <i>Transition Level</i>
<b>LEVEL 3</b> Good <i>CUI</i>
<b>LEVEL 2</b> Intermediate <i>Transition Level</i>
<b>LEVEL 1</b> Basic <i>FCI Only</i>

CMMC Model 2.0		
Level	Model	Assessment
<b>LEVEL 3</b>	<b>134</b> Requirements based on NIST SP 800-171 and 800-172	Triennial government-led assessment & annual affirmation
<b>LEVEL 2</b>	<b>110</b> Requirements aligned with NIS SP 800-171	Triennial third-party assessment & annual affirmation: Triennial self-assessment & annual affirmation for select programs
<b>LEVEL 1</b>	<b>15</b> Requirements	Annual self-assessment

## CMMC 2.0 Costs

There is no easy answer to how much CMMC 2.0 will cost DIB contractors. The total cost will vary depending on the sensitivity of data handled, the number of users in a system, the existing cybersecurity infrastructure, and the CMMC Level required by the specific contract.

Current contracts may not include CMMC as a requirement, and CMMC cannot be applied retroactively to contracts. However, once CMMC 2.0 is rolled out, compliance will be a prerequisite for all new DOD contracts. Without the requisite certification, contractors will not be able to bid on future contracts.



## Assessment/Certification Costs

Assessment costs are another layer of expense for any contractors seeking level 2 or 3 certification. This is the difference between compliance costs (cybersecurity investment) and certification costs. CMMC Levels 2 and 3 each require annual affirmations. Level 3 certification must be carried out every three years by government-led assessors. Level 2 certification must be carried out every three years by C3PAOs.

A subset of Level 2 designated contracts (contracts that include non-prioritized CUI), as well as Level 1 contracts, will be able to self-assess, meaning they will not be subject to certification costs.

The OUSD(A&S) anticipates that most contractors will need Level 2 certification. To ensure successful certification by 3PCAO or federal auditors, DIB contractors may also opt to conduct preliminary gap assessments prior to their certification audit. [CuickTrac](#) estimates CMMC gap assessments could be less than \$15,000 or more than \$35,000, based on current gap assessment costs for NIST 800-171 and ISO 27002 and the company's existing cybersecurity infrastructure .

One of the major objectives in transitioning from CMMC 1.0 to 2.0 is to reduce the overhead costs of certification, particularly for small businesses. OUSD(A&S) will publish comprehensive cost analyses for each level of CMMC 2.0 as part of rulemaking. However, these will only be estimates, since assessment costs will be set by the 3CPAOs, which function as separate, private-sector entities.

Additionally, not all cybersecurity costs will be included in the CMMC cost analysis, since many of the cybersecurity requirements are included in FAR 52.204-21 and DFARS 252.204-7012, which are already associated with government contracts.

[Certification costs will be considered allowable indirect costs](#), which can be billed to the DoD (at least for the first certification) . Current industry estimates place [CMMC 2.0 costs between \\$50,000 and \\$100,000](#), but these estimates have not been confirmed by the OUSD(A&S) .

## Infrastructure Investment and Remediation Costs

Companies with mature solutions for NIST 800-171 compliance will find that their overall CMMC compliance costs will be much lower. They have already invested in security hardening and access controls that answer many CMMC requirements.

Costs will be much higher for companies that need to implement brand new solutions. There will also be costs associated with infrastructure maintenance (recurring annual costs). These costs can be in the tens or even hundreds of thousands of dollars if it involves migrating from a public consumer product to a specialized compliant environment. Costs may be mitigated by opting instead for a self-hosted solution like FileCloud that provides guidance on compliant configurations and settings.



## FileCloud Supports CMMC 2.0

FileCloud is a hyper-secure content collaboration platform that provides compliance support in line with the shared responsibility model. This model was originally defined as a security framework for cloud service providers and customers.

The powerful governance, security, and access controls within FileCloud provide operational infrastructure that supports the organization of and access to content; as such, FileCloud is responsible for maintaining and securing the infrastructure itself. The end-user client is responsible for maintaining and securing data and other stored assets within and outside of FileCloud.

Implementing FileCloud can contribute to an efficient cybersecurity strategy and help streamline CMMC 2.0 certification.

### FileCloud-CMMC 2.0 Domain Checklist

CMMC requirements are organized into specific security domains. CMMC 1.0 included 17 domains. CMMC 2.0 has only 14 domains. Asset Management, Recovery, and Situational Awareness have been removed. Risk Management has been changed to Risk Assessment.



## Cybersecurity Maturity Model Certification (CMMC) 2.0

Domain	Requirements	How Does FileCloud Comply?
<b>Access Control (AC)</b>	<ul style="list-style-type: none"><li>• Establish system access requirements</li><li>• Control internal system access</li><li>• Control remote system access</li><li>• Limit data access to authorized users and processes</li></ul>	<ul style="list-style-type: none"><li>• Admin-controlled user profiles and user groups</li><li>• Granular file/folder permissions for users or groups</li><li>• Integrations: Active Directories (AD), LDAP, SSO, Network Shares, and NTFS permissions</li><li>• Data Leak Prevention (DLP) allows or denies file shares/downloads</li><li>• Role Based Access Control (RBAC) for admin users</li><li>• Access policies for connected remote devices</li></ul>
<b>Awareness and Training (AT)</b>	<ul style="list-style-type: none"><li>• Conduct security awareness activities</li><li>• Conduct training</li></ul>	<p>FileCloud provides complementary support to help optimize your FileCloud environment:</p> <ul style="list-style-type: none"><li>• FileCloud resource library on best security practices</li><li>• FileCloud University (training videos)</li><li>• Customer Support</li><li>• Professional Services</li></ul>





Domain	Requirements	How Does FileCloud Comply?
<p><b>Audit and Accountability</b></p>	<ul style="list-style-type: none"> <li>• Define audit requirements</li> <li>• Perform auditing</li> <li>• Identify and protect audit information</li> <li>• Review and manage audit logs</li> </ul>	<ul style="list-style-type: none"> <li>• Comprehensive audit logs (capture who accessed what data, with time stamps, IP addresses, and connected device information – who, what, when, where, &amp; how)</li> <li>• Audit log is unchangeable and can be exported for ease of review</li> <li>• SIEM integration</li> <li>• Hierarchical retention policies</li> <li>• Access/modification restrictions on specified records</li> </ul>
<p><b>Incident Response (IR)</b></p>	<ul style="list-style-type: none"> <li>• Plan incident response</li> <li>• Detect and report events</li> <li>• Develop and implement response to a declared incident</li> <li>• Perform post incident reviews</li> <li>• Test incident response</li> </ul>	<ul style="list-style-type: none"> <li>• Data governance dashboard displays potential rule violations (e.g., DLP, retention policies).</li> <li>• SIEM integration</li> <li>• Admin &amp; user-based workflow automation: workflows support automated report generation, device approval, and other tasks.</li> </ul>
<p><b>Media Protection</b></p>	<ul style="list-style-type: none"> <li>• Identify and mark media</li> <li>• Protect and control media</li> <li>• Sanitize media</li> <li>• Protect media during transport</li> </ul>	<ul style="list-style-type: none"> <li>• Integrated antivirus via ClamAV or ICAP protocol scans uploaded files</li> <li>• DLP provides granular control over data</li> <li>• In-transit encryption via HTTPS (SSL/TLS) protocols</li> </ul>



Domain	Requirements	How Does FileCloud Comply?
<p><b>Configuration Management (CM)</b></p>	<ul style="list-style-type: none"> <li>• Establish configuration baselines</li> </ul>	<p>FileCloud contains multiple configuration capabilities, including but not limited to:</p> <ul style="list-style-type: none"> <li>• Centralized device management</li> <li>• Content classification</li> <li>• DLP</li> <li>• Global policies</li> <li>• Device configuration policies</li> <li>• Customization</li> <li>• Data governance</li> <li>• User password enforcement</li> <li>• Private sharing permissions</li> <li>• Granular folder-level permissions</li> <li>• Configuration guides and examples (Support Documentation)</li> </ul>
<p><b>Identification and Authentication (IA)</b></p>	<ul style="list-style-type: none"> <li>• Grant access to authenticated entities</li> </ul>	<ul style="list-style-type: none"> <li>• Proprietary user authentication</li> <li>• AD/LDAP integration</li> <li>• Network shares integration</li> <li>• SSO &amp; 2FA</li> </ul>



Domain	Requirements	How Does FileCloud Comply?
<p><b>Maintenance (MA)</b></p>	<ul style="list-style-type: none"> <li>• Manage maintenance</li> </ul>	<ul style="list-style-type: none"> <li>• Workflows automate maintenance tasks within FileCloud; e.g., <ul style="list-style-type: none"> <li>◦ Deleting files after a specified amount of time</li> <li>◦ Disabling users who have not accessed FileCloud after a set number of days</li> </ul> </li> <li>• Automatic audit log trimming and export to a location defined by the administrator</li> <li>• Automatic backup capabilities (backupserver system)</li> <li>• Internal system scheduled tasks (CRON)</li> </ul>
<p><b>Personnel Security (PS)</b></p>	<ul style="list-style-type: none"> <li>• Screen personnel</li> <li>• Protect CUI during personnel actions</li> </ul>	<ul style="list-style-type: none"> <li>• Smart Classification + DLP automates classification and application of DLP rules that deny or permit downloading/sharing.</li> </ul>
<p><b>Physical Protection (PE)</b></p>	<ul style="list-style-type: none"> <li>• Limit physical access</li> </ul>	<p>Not Applicable</p>
<p><b>Risk Assessment (RA)</b></p>	<ul style="list-style-type: none"> <li>• Identify and evaluate risk</li> <li>• Manage risk</li> <li>• Manage supply chain risk</li> </ul>	<p>Not Applicable</p>



Domain	Requirements	How Does FileCloud Comply?
<p align="center"><b>Security Assessment (CA)</b></p>	<ul style="list-style-type: none"> <li>• Develop and manage a system security plan</li> <li>• Define and manage controls</li> <li>• Perform code reviews</li> </ul>	<p align="center">Not Applicable</p>
<p align="center"><b>Systems and Communications Protection (SC)</b></p>	<ul style="list-style-type: none"> <li>• Define security requirements for systems and communications</li> <li>• Control communications at system boundaries</li> </ul>	<ul style="list-style-type: none"> <li>• Separate login portals for admins and users</li> <li>• Granular access permissions for users or groups</li> <li>• DLP rules that permit or deny downloading/sharing of data</li> <li>• Encryption for data at rest and in transit</li> <li>• Configure FileCloud in FIPS mode (encryption + additional security features)</li> <li>• Client/customer key management support</li> </ul>
<p align="center"><b>System and Information Integrity (SI)</b></p>	<ul style="list-style-type: none"> <li>• Identify and manage information system flaws</li> <li>• Identify malicious content</li> <li>• Perform network and system monitoring</li> <li>• Implement advanced email protections</li> </ul>	<p align="center">Not Applicable</p>





## FileCloud-CMMC 2.0 Requirements Checklist

CMMC domains can be further broken down into explicit requirements, according to each CMMC certification level. These requirements have been mapped in a spreadsheet according to domain and certification level. This spreadsheet can be downloaded directly from the OUSD (A&S) CMMC website, under Documentation.

FileCloud provides the checklist below to easily review which requirements can be answered within FileCloud and which requirements must be met outside of the FileCloud environment.









## Access Control (AC)

CMMC 2.0	Details	FileCloud
Level 1		
AC.L1-3.1.1	<b>Authorized Access Control</b> Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	✓
AC.L1-3.1.2	<b>Transaction &amp; Function Control</b> Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	✓
AC.L1-3.1.20	<b>External Connections</b> Verify and control/limit connections to and use of external information systems.	✓
AC.L1-3.1.22	<b>Control Public Information</b> Control information posted or processed on publicly accessible information systems.	✓
Level 2		
AC.L2-3.1.3	<b>Control CUI Flow</b> Control the flow of CUI in accordance with approved authorizations.	✓





## Access Control (AC)

CMMC 2.0	Details	FileCloud
Level 2		
AC.L2-3.1.4	<b>Separation of Duties</b> Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
AC.L2-3.1.5	<b>Least Privilege</b> Employ the principle of least privilege, including for specific security functions and privileged accounts.	
AC.L2-3.1.6	<b>Non-Privileged Account Use</b> Use non-privileged accounts or roles when accessing nonsecurity functions.	
AC.L2-3.1.7	<b>Privileged Functions</b> Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
AC.L2-3.1.8	<b>Unsuccessful Logon Attempts</b> Limit unsuccessful logon attempts.	
AC.L2-3.1.9	<b>Privacy &amp; Security Notices</b> Provide privacy and security notices consistent with applicable CUI rules.	



## Access Control (AC)

CMMC 2.0	Details	FileCloud
Level 2		
AC.L2-3.1.10	<b>Session Lock</b> Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	✓
AC.L2-3.1.11	<b>Session Termination</b> Terminate (automatically) a user session after a defined condition.	✓
AC.L2-3.1.12	<b>Control Remote Access</b> Monitor and control remote access sessions.	✓
AC.L2-3.1.13	<b>Remote Access Confidentiality</b> Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	✓
AC.L2-3.1.14	<b>Remote Access Routing</b> Route remote access via managed access control points.	✓
AC.L2-3.1.15	<b>Privileged Remote Access</b> Authorize remote execution of privileged commands and remote access to security-relevant information.	✓



## Access Control (AC)

CMMC 2.0	Details	FileCloud
Level 2		
AC.L2-3.1.16	<b>Wireless Access Authorization</b> Authorize wireless access prior to allowing such connections.	N/A
AC.L2-3.1.17	<b>Wireless Access Protection</b> Protect wireless access using authentication and encryption.	N/A
AC.L2-3.1.18	<b>Mobile Device Connection</b> Control connection of mobile devices.	✓
AC.L2-3.1.19	<b>Encrypt CUI on Mobile</b> Encrypt CUI on mobile devices and mobile computing platforms.	✓
AC.L2-3.1.21	<b>Portable Storage Use</b> Limit use of portable storage devices on external systems.	N/A



## Awareness and Training (AT)

CMMC 2.0	Details	FileCloud
Level 2		
AT.L2-3.2.1	<b>Role-Based Risk Awareness</b> Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	N/A
AT.L2-3.2.2	<b>Role-Based Training</b> Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	N/A
AT.L2-3.2.3	<b>Insider Threat Awareness</b> Provide security awareness training on recognizing and reporting potential indicators of insider threat.	N/A



## Audit and Accountability (AU)

CMMC 2.0	Details	FileCloud
Level 2		
AU.L2-3.3.1	<b>System Auditing</b> Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	✓
AU.L2-3.3.2	<b>User Accountability</b> Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	✓
AU.L2-3.3.3	<b>Event Review</b> Review and update logged events.	✓
AU.L2-3.3.4	<b>Audit Failure Alerting</b> Alert in the event of an audit logging process failure.	✓
AU.L2-3.3.5	<b>Audit Correlation</b> Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	✓



## Audit and Accountability (AU)

CMMC 2.0	Details	FileCloud
Level 2		
AU.L2-3.3.6	<b>Reduction &amp; Reporting</b> Provide audit record reduction and report generation to support on-demand analysis and reporting.	✓
AU.L2-3.3.7	<b>Authoritative Time Source</b> Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	✓
AU.L2-3.3.8	<b>Audit Protection</b> Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	✓
AU.L2-3.3.9	<b>Audit Management</b> Limit management of audit logging functionality to a subset of privileged users.	✓





## Configuration Management (CM)

CMMC 2.0	Details	FileCloud
Level 2		
CM.L2-3.4.1	<b>System Baselineing</b> Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	N/A
CM.L2-3.4.2	<b>Security Configuration Enforcement</b> Establish and enforce security configuration settings for information technology products employed in organizational systems.	N/A
CM.L2-3.4.3	<b>System Change Management</b> Track, review, approve or disapprove, and log changes to organizational systems.	N/A
CM.L2-3.4.4	<b>Security Impact Analysis</b> Analyze the security impact of changes prior to implementation.	N/A
CM.L2-3.4.5	<b>Access Restrictions for Change</b> Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	N/A



## Configuration Management (CM)

CMMC 2.0	Details	FileCloud
Level 2		
CM.L2-3.4.6	<b>Least Functionality</b> Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	N/A
CM.L2-3.4.7	<b>Nonessential Functionality</b> Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	N/A
CM.L2-3.4.8	<b>Application Execution Policy</b> Apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software.	N/A
CM.L2-3.4.9	<b>User-Installed Software</b> Control and monitor user-installed software.	N/A









## Identification and Authentication (IA)

CMMC 2.0	Details	FileCloud
Level 1		
IA.L1-3.5.1	<b>Identification</b> Identify information system users, processes acting on behalf of users, or devices.	✓
IA.L1-3.5.2	<b>Authentication</b> Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	✓
Level 2		
IA.L2-3.5.3	<b>Multifactor Authentication</b> Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	✓



## Identification and Authentication (IA)

CMMC 2.0	Details	FileCloud
Level 2		
IA.L2-3.5.4	<b>Replay-Resistant Authentication</b> Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
IA.L2-3.5.5	<b>Identifier Reuse</b> Prevent reuse of identifiers for a defined period.	
IA.L2-3.5.6	<b>Identifier Handling</b> Disable identifiers after a defined period of inactivity.	
IA.L2-3.5.7	<b>Password Complexity</b> Enforce a minimum password complexity and change of characters when new passwords are created.	
IA.L2-3.5.8	<b>Password Reuse</b> Prohibit password reuse for a specified number of generations.	
IA.L2-3.5.9	<b>Temporary Passwords</b> Allow temporary password use for system logons with an immediate change to a permanent password.	



## Identification and Authentication (IA)

CMMC 2.0	Details	FileCloud
Level 2		
IA.L2-3.5.10	<b>Cryptographically-Protected Passwords</b> Store and transmit only cryptographically-protected passwords.	✓
IA.L2-3.5.11	<b>Obscure Feedback</b> Obscure feedback of authentication information.	✓

## Incident Response (IR)

CMMC 2.0	Details	FileCloud
Level 2		
IR.L2-3.6.1	<b>Incident Handling</b> Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	N/A
IR.L2-3.6.2	<b>Incident Reporting</b> Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	N/A



## Incident Response (IR)

CMMC 2.0	Details	FileCloud
Level 2		
IR.L2-3.6.3	<b>Incident Response Testing</b> Test the organizational incident response capability.	N/A

## Maintenance (MA)

CMMC 2.0	Details	FileCloud
Level 2		
MA.L2-3.7.1	<b>Perform Maintenance</b> Perform maintenance on organizational systems.	N/A
MA.L2-3.7.2	<b>System Maintenance Control</b> Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	N/A





## Maintenance (MA)

CMMC 2.0	Details	FileCloud
Level 2		
MA.L2-3.7.3	<b>Equipment Sanitization</b> Ensure equipment removed for off-site maintenance is sanitized of any CUI.	N/A
MA.L2-3.7.4	<b>Media Inspection</b> Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	N/A
MA.L2-3.7.5	<b>Nonlocal Maintenance</b> Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	N/A
MA.L2-3.7.6	<b>Maintenance Personnel</b> Supervise the maintenance activities of maintenance personnel without required access authorization.	N/A



## Media Protection (MP)

CMMC 2.0	Details	FileCloud
Level 1		
MP.L1-3.8.3	<b>Perform Maintenance</b> Perform maintenance on organizational systems.	N/A
Level 2		
MP.L2-3.8.1	<b>Media Protection</b> Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	N/A
MP.L2-3.8.2	<b>Media Access</b> Limit access to CUI on system media to authorized users.	✓
MP.L2-3.8.4	<b>Media Markings</b> Mark media with necessary CUI markings and distribution limitations.	✓



## Media Protection (MP)

CMMC 2.0	Details	FileCloud
Level 2		
MP.L2-3.8.5	<b>Media Accountability</b> Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	N/A
MP.L2-3.8.6	<b>Portable Storage Encryption</b> Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	N/A
MP.L2-3.8.7	<b>Removable Media</b> Control the use of removable media on system components.	N/A
MP.L2-3.8.8	<b>Shared Media</b> Prohibit the use of portable storage devices when such devices have no identifiable owner.	N/A
MP.L2-3.8.9	<b>Protect Backups</b> Protect the confidentiality of backup CUI at storage locations.	N/A



## Personnel Security (PS)

CMMC 2.0	Details	FileCloud
Level 2		
PS.L2-3.9.1	<b>Screen Individuals</b> Screen individuals prior to authorizing access to organizational systems containing CUI.	N/A
PS.L2-3.9.2	<b>Personnel Actions</b> Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	N/A

## Physical Protection (PE)

CMMC 2.0	Details	FileCloud
Level 1		
PE.L1-3.10.1	<b>Limit Physical Access</b> Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	N/A



## Physical Protection (PE)

CMMC 2.0	Details	FileCloud
Level 1		
PE.L1-3.10.3	<b>Escort Visitors</b> Escort visitors and monitor visitor activity.	N/A
PE.L1-3.10.4	<b>Physical Access Logs</b> Maintain audit logs of physical access.	N/A
PE.L1-3.10.5	<b>Manage Physical Access</b> Control and manage physical access devices.	N/A
Level 2		
PE.L2-3.10.2	<b>Monitor Facility</b> Protect and monitor the physical facility and support infrastructure for organizational systems.	N/A
PE.L2-3.10.6	<b>Alternative Work Sites</b> Enforce safeguarding measures for CUI at alternate work sites.	N/A



## Risk Assessment (RA)

CMMC 2.0	Details	FileCloud
Level 2		
RA.L2-3.11.1	<b>Risk Assessments</b> Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	N/A
RA.L2-3.11.2	<b>Vulnerability Scan</b> Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	N/A
RA.L2-3.11.3	<b>Vulnerability Remediation</b> Remediate vulnerabilities in accordance with risk assessments.	N/A



## Security Assessment (CA)

CMMC 2.0	Details	FileCloud
Level 2		
CA.L2-3.12.1	<b>Security Control Assessments</b> Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	N/A
CA.L2-3.12.2	<b>Plan of Action</b> Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	N/A
CA.L2-3.12.3	<b>Security Control Monitoring</b> Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	N/A
CA.L2-3.12.4	<b>System Security Plan</b> Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	N/A



## System and Communications Protection (SC)

CMMC 2.0	Details	FileCloud
Level 1		
SC.L1-3.13.1	<b>Boundary Protection</b> Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	N/A
SC.L1-3.13.5	<b>Public-Access System Separation</b> Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	N/A
Level 2		
SC.L2-3.13.2	<b>Security Engineering</b> Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	N/A
SC.L2-3.13.3	<b>Role Separation</b> Separate user functionality from system management functionality.	✓





## System and Communications Protection (SC)

CMMC 2.0	Details	FileCloud
Level 2		
SC.L2-3.13.4	<b>Shared Resource Control</b> Prevent unauthorized and unintended information transfer via shared system resources.	✓
SC.L2-3.13.6	<b>Network Communication by Exception</b> Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	✓
SC.L2-3.13.7	<b>Split Tunneling</b> Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	N/A
SC.L2-3.13.8	<b>Data in Transit</b> Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	✓



## System and Communications Protection (SC)

CMMC 2.0	Details	FileCloud
Level 2		
SC.L2-3.13.9	<b>Connections Termination</b> Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	N/A
SC.L2-3.13.10	<b>Key Management</b> Establish and manage cryptographic keys for cryptography employed in organizational systems.	✓
SC.L2-3.13.11	<b>CUI Encryption</b> Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	✓
SC.L2-3.13.12	<b>Collaborative Device Control</b> Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	N/A
SC.L2-3.13.13	<b>Mobile Code</b> Control and monitor the use of mobile code.	N/A
SC.L2-3.13.14	<b>Voice over Internet Protocol</b> Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	N/A



## System and Communications Protection (SC)

CMMC 2.0	Details	FileCloud
Level 2		
SC.L2-3.13.15	<b>Communications Authenticity</b> Protect the authenticity of communications sessions.	N/A
SC.L2-3.13.16	<b>Data at Rest</b> Protect the confidentiality of CUI at rest.	✓

## System and Information Integrity (SI)

CMMC 2.0	Details	FileCloud
Level 1		
SI.L1-3.14.1	<b>Flaw Remediation</b> Identify, report, and correct information and information system flaws in a timely manner.	N/A
SI.L1-3.14.2	<b>Malicious Code Protection</b> Provide protection from malicious code at appropriate locations within organizational information systems.	N/A



## System and Information Integrity (SI)

CMMC 2.0	Details	FileCloud
Level 1		
SI.L1-3.14.4	<b>Update Malicious Code Protection</b> Update malicious code protection mechanisms when new releases are available.	N/A
SI.L1-3.14.5	<b>System &amp; File Scanning</b> Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	N/A
Level 2		
SI.L2-3.14.3	<b>Security Alerts &amp; Advisories</b> Monitor system security alerts and advisories and take action in response.	N/A
SI.L2-3.14.6	<b>Monitor Communications for Attacks</b> Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	N/A
SI.L2-3.14.7	<b>Identify Unauthorized Use</b> Identify unauthorized use of organizational systems.	N/A



## Learn More

To learn more about cybersecurity, click the links below.

[How to Make Organizations Cyber Resilient in the Digital Frontier](#) →

[The Hidden Costs of Cybercrime](#) →

[About the CMMC](#) →

[The Evolution of FAR 52.204-21 to CMMC](#) →

[Cybersecurity Maturity Model Certification \(CMMC\) 2.0 Updates and Way Forward](#) →

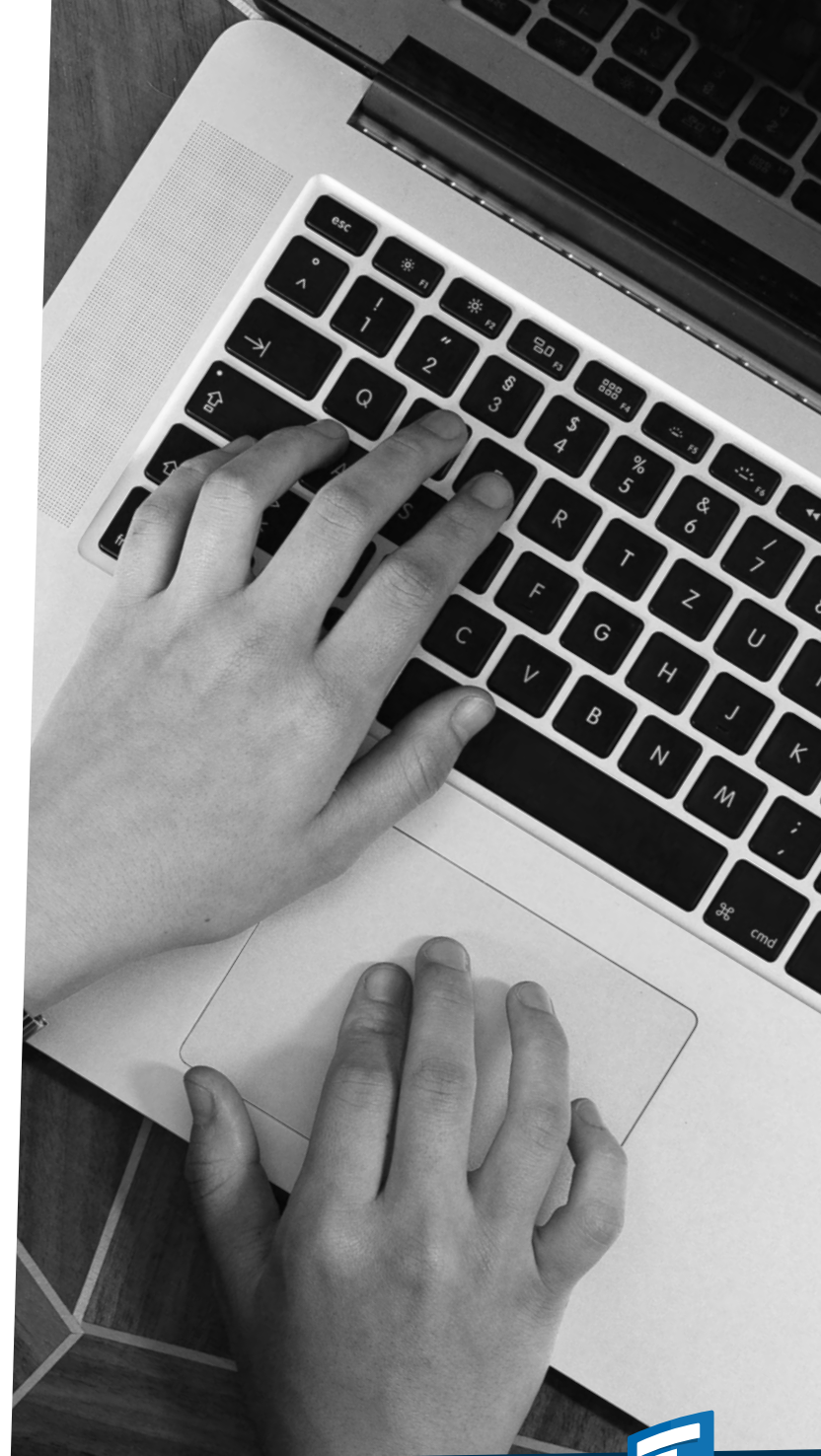
[CMMC 2.0 could take as long as two years to come online](#) →

[How Much Does CMMC Certification Cost?](#) →

[The Pitfalls of Factoring in Security and CMMC Costs](#) →

[CMMC Compliance 2.0 Guide](#) →

[CMMC Documentation](#) →



## Glossary of Terms

(in order of appearance)

**CMMC:** Cybersecurity Maturity Model Certification

**DIB:** Defense Industrial Base

**DoD:** Department of Defense

**FCI:** Federal Contract Information

**CUI:** Controlled Unclassified Information

**OSD(A&S):** Office of the Under Secretary of Defense for Acquisition and Sustainment

**UARC:** University Affiliated Research Centers

**FFRDC:** Federally Funded Research and Development Centers

**FAR:** Federal Acquisition Regulation

**DFARS:** Defense Federal Acquisition Regulation Supplement

**NIST:** National Institute of Standards of Technology

**SP:** Special Publication

**SPRS:** Supplier Performance Risk System

**DIBCAC:** Defense Industrial Base Cybersecurity Assessment Center

**ANPRM:** Advance Notice of Proposed Rulemaking

**CFR:** Code of Federal Regulations

**OMB:** Office of Management and Budget

**C3PAO:** Certified Third-Party Assessor Organization



# About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.



13785 Research Blvd, Suite 125  
Austin TX 78750, USA

**Phone:** U.S: +1 (888) 571-6480  
**Fax:** +1 (866) 824-9584



**1M+**  
USERS



**3000+**  
ENTERPRISES



**100+**  
RESELLERS



**90+**  
COUNTRIES

support@filecloud.com  
<https://www.filecloud.com>



US Army Corps  
of Engineers



Deloitte.

## Copyright Notice

© 2022 FileCloud. All rights reserved.

No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

