SecureCircle®

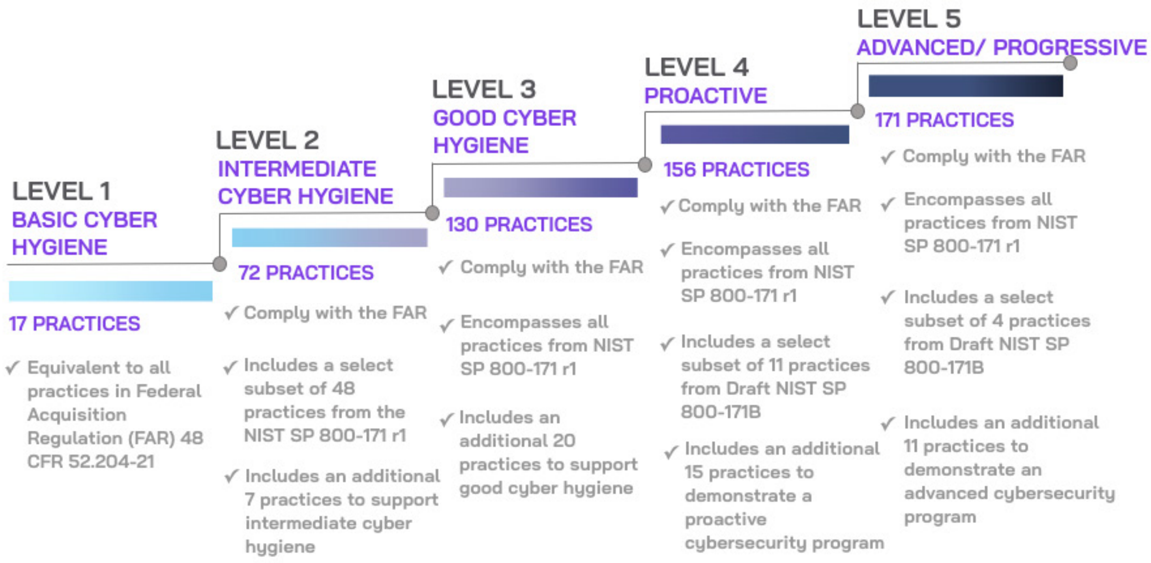
DATASHEET

Cybersecurity Maturity Model Certification

Cybersecurity Maturity Model Certification (CMMC) is the method the US Government uses to audit compliance with NIST SP 800-171. Various government agencies, including the Department of Defense (DoD) contractors, need to meet these requirements. CMMC replaces the Defense Industrial Base (DIB), which was not widely adopted.

Conservative estimates reveal up to 300,000 organizations will be in the scope of CMMC. Many of those are not traditional defense contractors. Many potentially impacted organizations are due to third parties' trickle-down effect that can affect the confidentiality of Controlled Unclassified Information (CUI) where it is stored, transmitted, or processed.

There are five levels of CMMC and each has its own specific set of practices that will be in scope during a CMMC audit.



LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

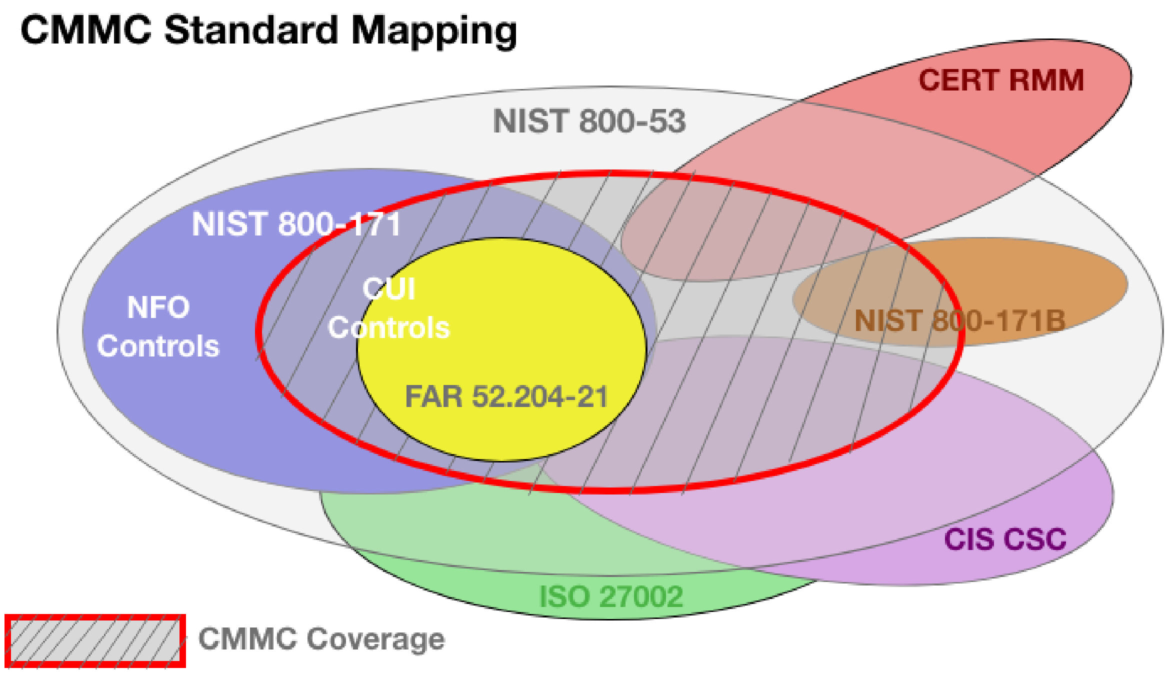
LEVEL 4
PROACTIVE
156 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED/ PROGRESSIVE
171 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

CMMC is not NIST 800-171

NIST 800-171 contains 110 CUI, and 63 Non-Federal Organization (NFO) controls. The NFO controls are included in Appendix E. To become compliant with NIST 800- 171, organizations need to comply with both the CUI and NFO controls.

CMMC only focuses on CUI controls. If NIST 800-171 is required, CMMC does not fulfill the requirement. Organizations that claim NIST 800-171 compliance incorrectly violate the False Claims Act (FCA). CMMC is a third-party validation to the necessary level of compliance.



CMMC requires a third party audit to gain certification. NIST 800-171 is a self-certification.

CMMC Includes 17 Domains

Access Control (AC)	Incident Response (IR)	Risk Managment (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

Why Do Customers Choose SecureCircle to Meet CMMC Requirements

- SecureCircle helps organizations meet over 40 controls and practices across eight domains needed to obtain Level 3 certification.

- Transparent and frictionless to users and applications. SecureCircle meets CMMC requirements without impacting users. This transparent approach means that user behavior does not need to change, and applications do not need to integrate in any way to take advantage of the control, and security SecureCircle delivers.

- Rapid and simple deployment. SecureCircle is a SaaS and endpoint agent architecture, enabling simple and fast deployment. No DLP rules to create or alerts to manage. Just define a Circle and allow users and applications to access data. There is no dependency on discovery or classification.

- Reduce cost and complexity. SecureCircle has a simple per-user pricing model that reduces our customers' costs.SecureCircle further reduces costs and reduces complexity by avoiding the need for multiple products, software integrations, and ongoing security controls administration.

SecureCircle Approach to CMMC & Data Security

SecureCircle's persistent data security and frictionless impact on users and applications allow SecureCircle to apply security to broad data segments rather than only securing the most critical data. To accomplish this, SecureCircle enables granular control and permissions for users, admins, groups, devices, applications, and networks. The combination of broad features and granular controls allow organizations to configure SecureCircle to meet security and compliance requirements.

SecureCircle enables organizations to meet CMMC controls and practices by configuring Circle policies, admin and user roles, network policies, admin and user groups, and integrate with central identity solutions and Syslog aggregation or Security Information and Event Management (SIEM) solutions.

SecureCircle is a client-server architecture and will function as long as client-server communication is possible. VPN and proxy connections are supported. Offline usage is configurable to balance security and compliance requirements with productivity. There are no limitations to the file size, file type, application, or host operating system.

Since data is persistently secured, SecureCircle doesn't need to block data transfer. Any data transfer, including removable devices or third-party cloud solutions, only transfers secured data. Organizations retain control of data regardless of location.

SecureCircle is aware of new applications that are attempting to access secured data in files. Default policies block new applications from accessing secured data. Administrators have full control over which applications can access secured data. Admins can also apply firewall-like inbound and outbound rules to applications.

Since traditional discovery or classification is not required, customers deploy in days and not months. Finally, SecureCircle removed the operational overhead that typically comes with legacy data loss prevention (DLP) tools. Since all data is secured by default, and security follows the data regardless of location, there is no need to create and maintain complex and error-prone DLP rules.

Table: SecureCircle Data Access Security Broker enables organizations to achieve the following CMMC requirements

Domain	Certification Number	CMMC Requirements
		Level 3
Access Control	AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion
	AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
	AC.3.019	Terminate (automatically) user sessions after a defined condition.
	AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote accesssessions.

Domain	Certification Number	CMMC Requirements
Level 3		
Audit & Accountability	AU.3.045	Review and update logged events.
	AU.3.046	Alert in the event of an audit logging process failure.
	AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
	AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.
ID & Authentication	IA.3.085	Prevent the reuse of identifiers for a defined period.
	IA.3.086	Disable identifiers after a defined period of inactivity.
Media Protection	MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.
Security Assessment	SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
	SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.
	SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.
	SC.3.190	Protect the authenticity of communications sessions.
	SC.3.191	Protect the confidentiality of CUI at rest.

Domain	Certification Number	CMMC Requirements
Level 2		
Access Control	AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.
	AC.2.006	Limit use of portable storage devices on external systems.
	AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.
	AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions
	AC.2.009	Limit unsuccessful logon attempts.
	AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
	AC.2.013	Monitor and control remote access sessions.
	AC.2.015	Route remote access via managed access control points.
	AC.2.016	Control the flow of CUI in accordance with approved authorizations.
Audit & Accountability	AU.2.041	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.2.042	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.
Configuration Management	CM.2.063	Control and monitor user-installed software.
ID & Authentication	IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.
	IA.2.079	Prohibit password reuse for a specified number of generations.
	IA.2.081	Store and transmit only cryptographically-protected passwords
Media Protection	MP.2.121	Control the use of removable media on system components.
Personnel Security	PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
Risk Management	RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	RM.2.143	Remediate vulnerabilities in accordance with risk assessments.

Domain	Certification Number	CMMC Requirements
		Level 1
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
	AC.1.004	Control information posted or processed on publicly accessible information systems.
ID & Authentication	ID.1.076	Identify information system users, processes acting on behalf of users, or devices.
	ID.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

What Data Can We Help You Secure?

At SecureCircle, our goal is to deliver genuinely frictionless security for our customers’ most valuable data. We focus on securing data persistently and transparently to provide business value for our customers. We are always looking for ways to improve our customers’ data security.

About SecureCircle

SecureCircle’s Data Access Security Broker (DASB) delivers a SaaS-based cybersecurity service that extends Zero Trust security to data on the endpoint. At SecureCircle, we believe frictionless data security drives business value for our customers. Instead of relying on complex reactive measures, we simply secure data persistently in transit, at rest, and even in use. End users operate without obstacles, while data is continuously secured against breaches and insider threats.

To Learn More

Contact your Data Access Security Broker expert at sales@securecircle.com or 408-827-9100

SecureCircle.com

4701 Patrick Henry Drive
Building 19, Suite B
Santa Clara, CA 95054
408-827-9100