nerdio

CMMC FAQ for IT professionals

Your technical guide to understanding CMMC and leveraging Nerdio Manager

nerdio

General questions

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a compliance framework developed by the Department of Defense (DoD) to enhance the cybersecurity posture of its supply chain. It mandates specific security practices and third-party certification to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

What are the CMMC levels, and what do they cover?

CMMC defines three levels of cybersecurity maturity, each building on the last:

- **Level 1 (Foundational):** Basic cyber hygiene practices to protect FCI, such as implementing antivirus software and ensuring authorized access to systems.
- **Level 2 (Advanced):** Compliance with the 110 security requirements outlined in NIST SP 800-171 to safeguard CUI.
- **Level 3 (Expert):** Advanced security controls aligned with NIST SP 800-172 to protect against advanced persistent threats (APTs).

Each level has specific technical requirements IT professionals must meet to achieve certification.

How do I know if I handle CUI?

Your prime contractors or subcontractors should address this, and it should also be specified by your contract in the DFARS 7012 clause. If a document contains CUI, it will be clearly marked with **CUI** in bold at the top.

Why is CMMC important for Defense Industrial Base customers?

IT professionals are responsible for implementing the technical controls required for CMMC compliance. Without proper implementation, organizations risk losing DoD contracts and exposing sensitive data. CMMC compliance also strengthens overall security posture and aligns organizations with industry best practices.

Why is creating a VDI enclave considered a great approach to CMMC?

After due diligence, it's often realized that not all employees handle CUI. For the portion of the organization that does, it is much more straightforward to implement resources to secure CUI by placing those workers in a VDI enclave. This approach makes the assessment scope much smaller and reduces the amount of resources required to go through an audit.

Building this infrastructure on top of the GCC/GCC High tenant and an Azure Gov Cloud subscription allows you to inherit all the security already put in place by Microsoft to handle CUI. This can often result in a shorter implementation ranging from 12 to 18 months down to just a few months.

> *"An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset"*

CMMC Scoping Guide Level 2, v. 2.13

When does this need to be done?

Short answer: Now.

On October 15, the DoD published the CMMC Final Rule, which kicked off a 60-day congressional review period. The current period as of this writing is the CMMC prep period. Prime contractors and subcontractors are rushing to figure out what to do. Now to Q2, 2025. After 10 years of delays, DIB primes and subs are now on high alert.

Phase 1 (Q2, 2025 to Q1, 2026): Self-assessments in applicable contracts • Level 1 and Level 2 self-assessment requirements will be included in all applicable* solicitations and contracts. At its discretion, the DoD may require certification instead of self-assessment.

Phase 2 (Q2, 2026 to Q2, 2027): Level 2 certification in applicable contracts • In addition to Phase 1 requirements, CMMC Level 2 certification requirements will be included in all applicable* solicitations and contracts.

Phase 3 (Q3, 2027 and beyond): Level 2 expands; Level 3 begins • Level 2 certification requirements expand to existing contracts exercising an option period. Contractors with existing contracts should expect CMMC requirements upon renewal. Level 3 certification requirements will appear in all applicable* solicitations and contracts.

nerdio

Technical questions

What are the key cybersecurity domains covered by CMMC?

CMMC focuses on 14 domains, including:

- **Access control (AC):** Enforce least privilege access and multifactor authentication.
- **Incident response (IR):** Develop a formalized incident response process.
- **Audit and accountability (AU):** Implement logging and monitoring for system access and activities.
- **System and communications protection (SC):** Encrypt data in transit and at rest using FIPS 140-2 validated cryptography.
- **Configuration management (CM):** Maintain secure configurations for hardware, software, and systems.

What is required for an SSP (system security plan)?

An SSP documents your organization's security infrastructure, controls, and configurations. It is a foundational requirement for CMMC certification and must include details, such as:

- System boundaries and architecture diagrams.
- A list of security controls implemented to meet CMMC requirements.
- Procedures for maintaining and monitoring security practices.

How can IT professionals prepare for CMMC audits?

- Conduct a **gap analysis** to compare current security practices with CMMC requirements.
- Develop a detailed SSP and POA&M (plan of action & milestones) for remediation efforts.
- Implement and document evidence for key controls, such as MFA, encryption, and vulnerability scanning.
- Use tools such as Nerdio Manager to centralize CIS Benchmark tracking and reporting.
- Create a secure VDI enclave using Nerdio to manage Azure Virtual Desktops in GCC/GCC High tenants with Azure GovCloud subscriptions.

nerdio

Nerdio-specific solutions

How does Nerdio Manager assist with CMMC compliance?

Nerdio Manager provides IT professionals with the tools needed to meet CMMC requirements efficiently, including:

- **CIS Hardened Images:** Deploy pre-configured, compliant virtual machines that align with CMMC security controls.
- **Secure Score Management:** Utilize centralized dashboards to identify vulnerabilities and track compliance progress.
- **Policy Automation:** Enforce CMMC-aligned security configurations across environments with pre-configured CIS Policy Baselines.
- **Role-Based Access Control (RBAC):** Implement granular permissions management to comply with access control requirements.
- **Audit Reporting:** Automate the generation of detailed compliance reports, reducing manual preparation for assessments.
- **GCC/GCC High Support:** Integrate seamlessly with Microsoft Government Community Cloud environments to ensure compliance in secure and regulated sectors.
- **Azure GovCloud Subscription Support:** Inherit the secure nature of Azure Government Cloud for CUI to build your secure AVD enclave, considerably reducing the assessment scope.

Can Nerdio Manager support higher levels of CMMC compliance (Level 2 and Level 3)?

Yes, Nerdio Manager includes features to address Level 2 and Level 3 requirements, such as:

- Enforcement of NIST SP 800-171 and SP 800-172 security practices.
- Advanced monitoring for configuration drift and policy enforcement.
- Tools to track and manage audit logs and access control configurations.

Can Nerdio be used in CMMC environments?

Yes, Nerdio is already used by top Microsoft ASO-G (Microsoft Agreement for Online Services - Government program) to serve up secure VDI enclaves by leveraging Azure Virtual Desktops in GCC High and Azure GovCloud regions.

While Nerdio does not handle or have access to any CUI, we have taken additional steps to set up support for our partners and customers who are looking to comply with ITAR requirements by having US personnel that support our DIB/CMMC 2.0 customers using our solutions.

nerdio

Practical implementation

What are the most critical technical controls to implement for CMMC compliance?

- **Access controls:** Implement MFA, limit access to authorized personnel, and enforce role-based permissions.
- **Data encryption:** Use FIPS 140-2 validated encryption for all sensitive data.
- **Continuous monitoring:** Deploy tools to detect and remediate vulnerabilities in real time.
- **Incident response:** Establish and test an incident response plan to ensure quick reaction to potential breaches.

What tools can IT professionals use to streamline compliance efforts?

IT professionals can leverage Nerdio Manager for:

- Automating the deployment of CIS Hardened Images and security policies.
- Tracking compliance metrics across multiple tenants from a centralized dashboard.
- Generating audit-ready reports to reduce manual preparation for third-party assessments.
- Managing secure GCC environments with ease.

Pro tips from Nerdio

- **Use automated policies:** Automate the deployment of CMMC-aligned configurations using Nerdio's pre-configured CIS Policy Baselines.
- **Track security metrics continuously:** Leverage Secure Score in Nerdio Manager to stay on top of vulnerabilities and ensure compliance across all systems.
- **Centralize your management:** Simplify complex compliance workflows by managing policies and configurations from a single platform.
- **Deploy secure virtual machines:** Use CIS Hardened Images in Nerdio Manager to save time on manual configuration and meet compliance requirements faster.
- **Centralize compliance across GCC:** Leverage Nerdio Manager's GCC support to simplify policy management and reporting for government tenants.

nerdio

CMMC compliance checklist for IT professionals

- [ ] Conduct a detailed gap analysis against NIST SP 800-171 or SP 800-172 controls.
- [ ] Develop a system security plan (SSP) and plan of action & milestones (POA&M).
- [ ] Implement technical controls, such as MFA, data encryption, and logging.
- [ ] Establish continuous monitoring for vulnerabilities and compliance drift.
- [ ] Schedule an audit with a Certified Third-Party Assessment Organization (C3PAO).
- [ ] Use automation tools, such as Nerdio Manager, to streamline policy enforcement and reporting.

Why CMMC compliance matters

CMMC certification is no longer optional for DoD contractors and supply chain organizations. By adhering to CMMC standards, IT professionals ensure the protection of sensitive data, maintain eligibility for government contracts, and enhance their organizations' overall cybersecurity resilience.

For more information about Nerdio Manager and how it supports your CMMC compliance journey, visit getnerdio.com.

About Nerdio

Nerdio is a leading provider of powerful, simplified cloud management solutions for businesses of all sizes. Trusted by managed service providers (MSPs) and enterprise IT departments alike, Nerdio equips organizations with seamless, cost-effective management tools for Azure Virtual Desktop (AVD), Windows 365, and comprehensive Modern Work solutions.

With thousands of customers worldwide, Nerdio accelerates cloud adoption, enabling companies to thrive in an era of hybrid work by providing modern, future-proof technology that adapts to evolving workplace needs.

For more information, please visit **www.getnerdio.com**.

nerdio

WEB www.getnerdio.com
EMAIL hello@getnerdio.com

EB52325005